Faster Payments QIAT

Proposer: *World Currency USA, Inc*

February 21, 2017

**TABLE OF CONTENTS**

Original Proposal 2

Q&A Response 69

Draft QIAT Assessment 85
   (Includes proposer comment in Appendix A & B) 99

Task Force comments 102

Proposer response to Task Force comments 108

Final QIAT Assessment 109
Final Version
March 2, 2016

Faster Payments Task Force Proposal

FAST Payments Network Solution

April 29, 2016

Submitted by:

Michael Ruccolo, World Currency USA, Inc.
Bill Toffel, World Currency USA, Inc.

[Note: If submitted jointly by multiple parties, list all parties separately.]
CONTENTS

Background ..................................................................................................................................... 4
Purpose of the Template and Instructions for Use.............................................................. 5
  Proposal Review Process ................................................................................................. 5
  Instructions for Submission and Proposal Review Process Timeline ......................... 6
  Legal Considerations .................................................................................................... 7
Proposal Template ............................................................................................................... 9
Executive Summary .............................................................................................................. 9
Use Case Coverage ............................................................................................................. 12
  Supported Use Case Coverage Summary ................................................................. 12
  Cross-border Use Case Coverage (If Applicable) ....................................................... 13
  Proposal Assumptions (Optional) ............................................................................. 14
Part A: Detailed End-to-End Payments Flow Description .............................................. 15
  Part A, Section 1: Solution Description ..................................................................... 15
    1. Initiation ............................................................................................................. 16
    2. Authentication .................................................................................................. 17
    3. Payer Authorization ........................................................................................ 18
    4. Approval by the Payer’s Provider ................................................................. 19
    5. Clearing ............................................................................................................. 19
    6. Receipt .............................................................................................................. 20
    7. Settlement ....................................................................................................... 20
    8. Reconciliation .................................................................................................. 21
  Part A, Section 2: Use Case Description ................................................................... 22
  Part A, Section 3: Use Case by Effectiveness Criteria .............................................. 30
Part B: Business Considerations ..................................................................................... 32
  1. Implementation Timeline .................................................................................. 32
  2. Value Proposition and Competition .................................................................. 34
  3. Integration Effort ................................................................................................ 39
Part C: Self-Assessment Against Effectiveness Criteria ............................................... 45
1. Ubiquity ................................................................................................................... 46
2. Efficiency ............................................................................................................... 48
3. Safety and Security ............................................................................................... 51
4. Speed (Fast) ......................................................................................................... 56
5. Legal Framework ................................................................................................. 58
6. Governance .......................................................................................................... 60
BACKGROUND

Strategy 2 of the Federal Reserve’s Strategies for Improving the U.S. Payment System paper is to “Identify effective approach(es) for implementing a safe, ubiquitous, faster payments capability in the United States”. The Faster Payments Task Force was created to support this strategy and has designed the Faster Payments Effectiveness Criteria (Effectiveness Criteria) and process for assessing alternative faster payments proposals.\(^1\) The Effectiveness Criteria is consistent with Strategy 2, as well as the broader set of “desired outcomes” set out in the Strategies Paper. These desired outcomes include:

**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.

**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.

**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.

**International:** Better choices for U.S. consumers and businesses to send and receive convenient, cost-effective and timely cross-border payments.

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

All proposals submitted through the Task Force’s assessment process will be assessed against the Effectiveness Criteria to determine how well solutions can achieve the desired outcomes associated with improving the U.S. payments system.

---

\(^1\) “Proposal” is defined in the [Glossary of Terms](#) as, “The written document that provides a detailed description of a faster payments solution, and demonstrates how it meets the Effectiveness Criteria for a faster payments solution”.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
PURPOSE OF THE TEMPLATE AND INSTRUCTIONS FOR USE

This proposal template has been developed to assist proposers in detailing their proposal for a full end-to-end faster payments solution. The template is designed to increase the consistency of information provided by proposers, as well as to provide the breadth and depth of information needed for the Qualified Independent Assessment Team (QIAT) to understand and assess a proposal against the Effectiveness Criteria. Proposers submitting proposals for assessment by the QIAT should use this template and complete all parts and sub-sections as described in the instructions.

This template includes three parts. Part A requires proposers to describe and illustrate (via a flow chart) what the solution does at each stage of the end-to-end payments process (from initiation of the payment through to the reconciliation of the payment). This description should be provided for the solution overall, as well as for each use case that is supported by the solution. Proposers will also be required to complete a table indicating which parts of the criteria each use case addresses (for example, the solution may enable contextual data capability for business-to-business payments, but not for person-to-person payments). Part B requires proposers to describe business considerations for the solution. These business considerations include: a detailed timeline to achieve initial implementation and then to achieve ubiquity; the intended value proposition of the solution and how it supports competition; and integration considerations. The detail in Part B will help the QIAT understand the feasibility of the solution and will help support its assessment against the Effectiveness Criteria. Part C requires proposers to provide a self-assessment and justification of how the solution meets each of the criteria outlined in the Effectiveness Criteria.

Proposers should refer to the Effectiveness Criteria when completing all parts of the proposal template.

Proposal Review Process

Once a proposal has been submitted, a qualitative assessment of the proposal against the Effectiveness Criteria will be conducted by the QIAT. During the assessment process, the

---

2 A full end-to-end faster payments solution (or “Solution”) is defined in the Glossary of Terms as, “The collection of components and supporting parties that enable the end-to-end payment process. A faster payments solution might include new components, the adaptation of existing components, and/or a combination of the two.

- Components include any of the following:
  - Rules, standards/protocols, and procedures
  - Physical or technical infrastructure, networks, systems and other resources needed by all parties to use or enable the rules, standards/protocols and procedures
  - Centralized or shared services, if any
  - Legal framework and enforcement mechanisms
- Parties include any of the following:
  - Governing bodies, operators, depository institutions, non-bank account providers and third-party service providers”.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
The proposer will have the opportunity to provide additional information and/or a response to the assessment. The proposer may also choose to withdraw its proposal at any point in during this initial assessment meaning that the proposal will not be shared with the Faster Payments or Secure Payments Task Forces. No confidential or proprietary information should be shared in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report.

Following the completion of the QIAT’s assessment and the compilation of any responses received from the proposer, the assessment will be provided to the Faster Payments Task Force for review. The proposal will be reviewed in its entirety, including the assessment and the proposer response, and Task Force members may offer comments to the proposer and the QIAT. Similarly, the Secure Payments Task Force will review the proposal and provide comments on the security-related aspects to the proposer and the QIAT. The proposer may respond to Task Force comments and may revise its proposal for final QIAT review. The proposer may also choose to withdraw its proposal at this point meaning that the proposal will not be published as part of the final report.

The QIAT will finalize its assessment of the revised proposal with consideration given to comments by both Task Forces. Once the assessment has been finalized, the proposal, QIAT final assessment, and Task Force comments will be published in a final report along with corresponding material for all other solution proposals that underwent and completed the proposal review process.

**Instructions for Submission and Proposal Review Process Timeline**

Proposals should be provided in Word or PDF format, submitted on 8½ x 11 inch paper with 1 inch borders and Times New Roman font size 12. It is advised that proposers limit the total length of each proposal (including optional appendix) to a maximum of 200 pages. Proposers choosing to attach an optional appendix should ensure that it is highly organized with a table of contents and any reference to the appendix in the main body of the text should be clearly cross referenced. As noted above, the QIAT will have a dialogue with proposers and will request additional explanation if required. Proposals should be written to the primary audience of the QIAT, and the Faster Payments and Secure Payments Task Forces.

All inquiries regarding the proposal template and submission process should be directed to: FasterPaymentsTaskForce@chi.frb.org.

Instructions providing details on where proposals are to be submitted will be provided in a separate communication prior to the submission window opening on April 1.

The following table outlines the proposal assessment process and timeline. Key dates for proposers are indicated in bold type.
### Timeline and key dates

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Proposers to submit proposals</strong></td>
<td><strong>Proposal submission window open from 9am ET April 1, 2016 to 5pm ET April 15, 2016</strong></td>
</tr>
<tr>
<td>2. <strong>Draft 1 of QIAT assessment and discovery period between QIAT and proposers</strong></td>
<td>Conducted from April 15, 2016 to July 7, 2016</td>
</tr>
<tr>
<td>3. <strong>Proposers to provide written response to QIAT assessment or notification of decision to withdraw</strong></td>
<td>Due no later than 5pm ET August 9, 2016</td>
</tr>
<tr>
<td>4. <strong>Task Force review of proposal assessments commentary period</strong></td>
<td>Conducted from August 10, 2016 to October 4, 2016</td>
</tr>
<tr>
<td>5. <strong>Proposer to submit final revised proposal, and written response to Task Force comments or notification of decision to withdraw prior to public release</strong></td>
<td>End-October 2016</td>
</tr>
<tr>
<td>6. <strong>Final QIAT assessment provided to proposers</strong></td>
<td>November 2016</td>
</tr>
<tr>
<td>7. <strong>QIAT report of all fully assessed proposals including Task Force commentary and proposer responses</strong></td>
<td>November 29, 2016</td>
</tr>
</tbody>
</table>

### Legal Considerations

All submissions are at the discretion of the proposer or proposers, and are subject to the terms outlined in the Faster Payment Task Force Proposal template and the terms of the Faster Payment Task Force Participation Agreement. Please limit your responses to matters reasonably necessary to the creation, development, and deployment of your proposed solution.

All Faster Payments Task Force Members who contribute to a proposal are considered to be proposers, and a proposal should identify all Task Force Members who have contributed. If a Secure Payments Task Force Member contributes to a proposal, that Secure Payments Task Force Member should sign a Faster Payments Task Force Agreement and be included as a proposer.

Proposers should identify the proprietary intellectual property contained in its proposal. This identification should include whether the proposer owns the intellectual property or whether the intellectual property has been licensed or will require licensing from another entity (in the event the proposer has licensed technology from another entity), the terms the proposer will license its intellectual property under and the terms of license(s) required from other entities. These terms could include FRAND, royalty bearing, or non-royalty bearing, by way of example. Such disclosures should be made under Part C, sub-section 5 “Legal Framework” (justification for L.5, Intellectual property criterion), which asks whether a proposal has undertaken or will undertake a due diligence review for the subject matter disclosed by a proposal, and an approach
to resolve or manage any risks that arise from third-party intellectual property rights implicated by a proposal. In making these disclosures, proposers should identify any technology that is disclosed by its proposal, which the proposer has knowledge potentially infringes or misappropriates the intellectual property of any other entity or person, and the basis on which the proposer has this knowledge.

If a proposer does not currently have access to Federal Reserve System (FRS) services referenced in a proposal or the proposal relies upon new or the expansion of existing FRS services, the proposal must clearly acknowledge that the FRS has not in any way committed to provide the services to the proposer.

Proposers are reminded of their obligations to comply with applicable anti-trust laws in preparing their proposals. Proposers should not share confidential or proprietary information in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report. While all information contained in a proposal is ultimately at the discretion of the proposer(s), if a proposer inadvertently includes confidential or proprietary information in a proposal, the proposer should immediately notify the QIAT.
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).

This proposal describes a unified full stack front-end and back-end payments solution (“Solution”) to allow for the secure inter-connection of the world’s banking institutions in order to provide a single mechanism for money movement. The proposer is World Currency USA, Inc. (“WCUSA”).

The Solution specifically aims to address the full payments life-cycle across all desired use cases (B2B, B2P, P2B, and P2P), with an expectation that a certain Party A will seek to transfer funds to or from themselves with a second Party B as quickly, efficiently, and inexpensively as possible. Party A could be a business or individual, and similarly Party B could be a business or individual. The Solution will address all regulatory guidance for both domestic and international electronic transfers, namely fully satisfying the adoption of Dodd-Frank and Regulation E.

WCUSA has constructed a Software-as-a-Service (SaaS) model for banks to connect into and conduct payment operations, with opportunity to phase in extensible to Platform-as-a-Service (PaaS) capabilities over time.

When considering the current context of both domestic and cross-border applications, payments models now consist of widely disparate approaches, technologies, workflows, operational considerations, and compliance hurdles. Domestically, we primarily rely on the Federal Reserve System (the “Fed”) to manage the facilitation of NACHA-formatted messages back and forth allowing U.S. endpoint banks to clear and settle funds with the Fed before they are ultimately routed to their final banking destination. Internationally, we may also rely on specially designated NACHA-formatted messages that supply limited Fed reach to a small subset of the international banking community. International systems external to the Fed typically involve the SWIFT messaging network to deliver routing information to foreign banks.

Our Solution improves on the current models by providing an alternative parallel connection network for global endpoint banking systems, also including the Fed, to each agree on
connectivity, communications, workflow, and settlement processes. The Solution promotes a fundamental shift in the way that payments handled, allowing a single common system to integrate foreign and domestic payments with simplicity for the endpoint bank. We consolidate the notion of domestic ACH and Wire transfers into this singular payments Solution, as well as the inclusion of cross-border capabilities for any and all banking and financial institutions worldwide.

In order to ensure that the worlds’ existing payments platforms continue without disruption, this Solution is designed to be used in parallel, invoking a “least cost routing” paradigm to ensure that this end-to-end system will try to route payments initially through this newly proposed mechanism, but also gracefully handle using existing payments platforms (such as the ACH network) in the event that is the only achievable or preferred method. The Solution’s front-end system will also allow for integrations with other payment providers to further ensure this end-to-end solution.

The Solution utilizes a membership model to allow itself to grow and mature before any future formalized adoption process. Similar to other networks such as SWIFT, participants will be considered “Members”. Each Member will act as an autonomous node within the Solution. The temporarily moniker for the network is “FAST”, and Members will be considered FAST Members. This membership model is key as it provides the direct endpoints where payments can be routed. Members are contractually bound participants.

A FAST Network Central Authority must oversee certain aspects of the Solution, including the vetting of Members and the authoritative control mechanism over enforcing the Member rules of engagement. It is recommended that the Central Authority be representatives of various central banks and/or other banking institutions to promote comfort with adoption, especially in foreign countries that may be skeptical of a solely U.S.-controlled platform.

Once vetted, FAST Members are connected to one another via their access to a web based front-end platform, effectively providing a segregated and secure extranet among Members.

Payments are originated in the following manner:

- A Member will access their authorized user account for the front-end platform and designate to send or receive either a domestic and/or foreign payment on behalf of their customer. The recipient’s banking institution will have a unique FAST identifier.
  - If the recipient is not a FAST Member, then the Solution must rely on other providers that the Member has in place (such as Fed for ACH and Wires, correspondent relationships for domestic and/or cross-border, etc.) to route the payment appropriately.
  - Otherwise:
After all compliance disclosure and OFAC checks are performed by the Member utilizing the front-end platform, the payments are sent to a queuing mechanism for processing.

Baseline features include:

- Member network based approach to including and growing bank participation within this Solution.
- Standalone web-based front-end platform for banks provides capabilities for centralized management of customers, price and fee schedules, compliance disclosures, and transaction origination and management.
- Standalone web-based front end that banks may elect to express to their end-user customer, allowing customers to initiate and view transactions in real-time based on permissions and control settings.
- Ability to route transactions utilizing the described Solution flow where available and desired, while additionally supporting integration points to leverage alternative existing payment systems (i.e. ACH, etc).
- Unifies the approach and mechanism for both domestic and cross-border payments into a single system.
- Cross-border system will first take advantage of intelligent matching algorithms where currencies will be sourced by other peer network members before being sent to the currency exchange market for fulfillment.
- Provides real-time confirmation of funds by receiver, instantly viewable to the originator.
- Through optional integration with a Member-procured third-party provider, the system may also support payments via alternate mechanisms such as Bitcoin.

Money flow consists of entry changes in a centralized register which behaves as the accounting differentials required by the banks to their in-process account. The messaging is pushed from the originator to the system where it is processed and subsequent accounting messages are recorded and available for appropriate parties. Members can access messages through their front-end platform, and additionally RESTful web service technologies will be used to allow other bank systems to query for messages. WORM (write once read many) style transaction logging allow the FAST central authority to investigate and resolve any disputes. This register may also be used by regulators and internal / external audit to prove the accuracy of the in-process accounts at each Member institution.
**USE CASE COVERAGE**

**Supported Use Case Coverage Summary**

In the table below, identify (by entering a “Y” or an “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>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Business to Person (B2P)</td>
<td>Y</td>
<td>N</td>
<td>The solution assists business and governments to make payments. Payments supported include: social security, government pensions and employee wages.</td>
<td>Note that the solution targets regular income payments to individuals. It would not be suitable for all types of business-to-person payments, such as ad hoc legal settlement payments or medical insurance claims.</td>
</tr>
<tr>
<td>Business to Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>The solution assists businesses to make payments to other businesses, which may include payments to a vendor for goods and services.</td>
<td>Originator business and Receiver business requires a bank account.</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>This solution assists businesses to make payments to individuals, which may include refunds to individuals or employee wages.</td>
<td>Originator business and Receiver individual requires a bank account.</td>
</tr>
</tbody>
</table>
## Supported use case coverage summary

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>This solution assists individuals make payments to businesses, which may include bill payments.</td>
<td>Originator individual and Receiver business requires a bank account.</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>This solution assists individuals make payments to individuals, which may include settling personal debts.</td>
<td>Originator individual and Receiver individual requires a bank account.</td>
</tr>
</tbody>
</table>

### Cross-border Use Case Coverage (If Applicable)

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>Cross-border use case coverage</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>Potentially all</td>
<td>Jurisdictions in the denominated currency of any approved FAST Member are instantly available. Other currencies are dependent on the reach of the FX providers.</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Potentially all</td>
<td>(same as B2B)</td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Potentially all</td>
<td>(same as B2B)</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Potentially all</td>
<td>(same as B2B)</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.

- The Federal Reserve System (FRS) has not in any way committed to provide the services to the proposer, WCUSA.
- The FX Provider(s) referenced within this Proposal have not in any way committed to provide services to the proposer and/or the FAST Network.
- WCUSA owns certain intellectual property rights to technology and business methods used throughout this Proposal:
  - All references to the design, features, and technology of the web based front-end platform is based on the existing WCUSA “FXStudio” product and platform (both front-end and back-end).
  - All references to the design, features, and technology of the web based customer-facing front-end platform is based on the existing WCUSA “FXCenter” product and platform (both front-end and back-end).
- Michael Ruccolo, CEO of WCUSA and member of the FPTF, owns intellectual property rights to business methods used throughout this Proposal. All references to business methods filed within the following issued patents are protected property:
  - U.S. Patent #8,121,923 (https://www.google.com/patents/US8121923)
  - U.S. Patent #8,301,533 (https://www.google.com/patents/US8301533)
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 of 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).3 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

---

3 Definitions of some of the terms used below are either defined in the Effectiveness Criteria or in the Glossary of Terms.
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 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 pre-requisites or limitations to initiating or receiving a payment (e.g., enrollment,) and, if applicable, how those pre-requisites 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).

Banks and financial institutions must enroll and be approved by the FAST central authority prior to becoming Members. The enrollment process is a necessary vetting step to ensure that the proper boiler plate institution information is on file (official name, address, contacts, ABA, SWIFT, etc.), that the institution is a properly regulated entity within its domiciled region, that the institution has been presented and accepted all of the rules, expectations, and instructions of membership, and to ensure that the institution has agreed to be bound to any legal documentation.

Upon acceptance, the Member is issued with user account credentials to the web-based front end portal which will act as their primary conduit. At a minimum, there is nothing for the
institution to install or maintains, other than an existing Internet connection. Additional security measures may be implemented, as well as additional integration points into other providers, core systems, cash management systems, compliance and transaction monitoring systems, and/or other endpoints as may be required by the institution.

The bank will additionally need to create a segregated In-Process account acting as the conduit between the FAST Member network and their internal accounting system. Suggested training and documentation will be provided to assist the bank in addressing any differentials in operational logistics.

The enrollment process is stripped down to bare essentials, the technical implementation extremely easy, and the bank operational impact should be minimal with focus surrounding a single account. All are designed to be as simple as possible to optimize accessibility, usability, predictability,

All personally identifiable information will be encrypted by force both in-transit and at rest in the data model. SSL encryption technologies with issued certificates will secure the transmission of data to and from each individual Member to the system.

In the event of cross-border payments, currency exchange rates are presented to the customer prior the authorization of the transaction.

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).

Access to the front-end platform will consist primarily of user access controls. Users will authenticate to the platform by presenting a unique identifier of the Member, a unique username, and a password that is secret only to the user. If desired by the Member, multi-factor authentication schemes may be implemented to enhance the access control capabilities (Google Authenticator, Authy, SMS-based). Members may further restrict access from specific IP addresses.

Authenticated users will be presented with a token which will live with them through the duration of their session. With each functional request this token will be passed to the back end and evaluated for identity.
Access to any API services will consist of a slightly different authentication paradigm. Member level connectivity between the Member and the technology platform will be maintained via simple RESTful web service calls, ensuring development simplicity. Member organizations will authenticate with a unique identifier issued to their organization and a secret key known only to the organization. This information will be presented with every authentication request.

In addition, the specific user requesting access to the web service resource will also present username and password credentials. All information will be evaluated to determine proper authentication, and a session token will be issued and must be presented in every subsequent call.

Session tokens can be revoked at any time by properly permissioned administrator users within the front-end platform, forcing the user to re-authenticate before continuing.

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).

The payer has two ways in which they can initiate and authorize a payment: via instructing the Member bank, or via direct initiation through a customer facing front-end platform if the Member bank has allowed them to gain entry.

The first scenario is via the Member (i.e. phone, fax, visit to a Member branch office). In this scenario the payer (business or individual) declares their intention to initiate a payment directly to the Member and the Member initiates the request within their front-end platform. The front-end platform allows the Member to follow an easy wizard-based transaction entry process consisting of (1) data entry, (2) customer verification, and (3) back-end verification/release. At step 2 the Member will be presented with all compliance disclosure information to satisfy successful payer authorization. It is up to the Member to keep the necessary proof as part of their internal policies.

The second scenario is if the Member bank has granted the payer direct access to the customer facing front-end system allowing them to originate transaction requests for themselves. The authorization is handled by duly authenticated customer user submitting the
request. That authorization is backed by the agreement of an initial EULA and subsequent disclosure language presented by the platform at the time of transaction. Transaction entry is similar, with an easy-based transaction wizard to guide the end user. In all cases the payer is authorizing the immediate and irreversible remittance of funds.

4. **Approval by the Payer’s Provider**

   Detail the process for approval of the payer’s provider (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.\(^4\) 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).

   Depending on the settings, the Member will authorize the transaction via the front-end platform before it is released. This affords Members the ability of a last look before releasing a payment under their Member name. Under certain circumstances the Member may opt to have the system auto-book the transaction. This process is as easy as re-keying the dollar amount and clicking on a button to release the payment, however, it provides an essential level of control by the Member institution.

5. **Clearing**

   Detail the process for the exchange of relevant payment information between a payer’s and a payee’s providers (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.

\(^4\) The completion of payment initiation is defined as just following payer authorization to their provider, or just following confirmation by the payer’s provider that pre-authorization exists for a given payment.
Clearing of all “In Network” Members is facilitated through the establishment use of a FAST In-Process clearing account located at each Member location. Similar to a Fed sweep account, this is the gateway account that is debited and credited providing the link between the depositor’s bank account and the FAST Network.

The Solution will have its own payment messaging format standards to be developed and published by the FAST Network Central Authority. The messaging format will address value and routing information.

All “In Network” payments are cleared by debit and/or credit instructions provided by the technology platform to the Member.

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).

After the transaction has completed, the receipt may be retrieved within the secured front-end platform. The receipt is available immediately upon the recipient accepting the payment.

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).

**Settlement** occurs once the receiving Member acknowledges the acceptance of the incoming payment. Since this is a positive validation measure, feedback of confirmed receipt can be communicated in real-time to both the originator and the receiver.

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).

The Member must reconcile its FAST In-Process clearing account activity against the centralized log file maintained by the FAST Network Central Authority, and accessible to the Member through the front-end platform.

Because of the existence of this offsite centralized “write once read many” log of each transaction status checkpoint, the Member reconciliation can be performed against this independent master log of transactions.

The Member can also easily present proof of the centralized transaction log to their regulatory authority for use in audit or third-party assessment of the Member bank’s accuracy and controls in this area.
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.

Please see Appendix A for workflow illustrations referenced below.

Figure 1a – Use Case Stakeholders

(1) “Member 1” represents a FAST Member bank with accounts denominated in USD.
(2) “Member 2” represents a FAST Member bank with accounts denominated in USD.
(3) “Member 3” represents a FAST Member bank with accounts denominated in EUR.
(4) “Non-Member 1” represents a bank that is not a FAST member with accounts denominated in USD.
(5) “Non-Member 2” represents a bank that is not a FAST member with accounts denominated in EUR.
(6) “Queuing Service Back-End” is the technology platform.
(7) “FAST Network Central Authority” is the oversight and clearing arm of the organizational structure. This will likely be the Federal Reserve Bank, but may be a separate legal structure.
(8) “FedACH” is the pre-existing Federal Reserve payments network.
(9) “FX Prov” is the network of foreign exchange providers that the Central Authority has lined up to backstop FX transactions.

**Figure 1b – Domestic Payments Workflow (In Network)**

**SCENARIO:** Payer A, an account holder of Member 1 bank, is looking to remit 100 USD to Beneficiary A, an account holder of Member 2 bank. Both Member 1 and Member 2 are valid FAST Network Members. Total expected time between Payer A transaction request and Beneficiary A funds availability is less than 15 minutes.

1. The transaction process begins with a request from Payer A to send 100 USD. Payer A interacts with Member 1 to initiate the payment. Member 1 keys the information into the web-based front-end platform. Alternatively, if authorized by Member 1, Payer A may directly enter the payment request into their own customer-facing portal. If known, Member 1 will enter the FAST Member unique identifier of the recipient bank, otherwise the front-end will attempt a lookup of the information to determine whether Member 2 is “in network”, which in this scenario is true. The front-end handles the Member 1 control environment for authorizing payments, its customer disclosures, and guides Member 1 through searching against OFAC prior to release. If desired, the front-end platform also guides Member 1 through assessing and collecting any transaction fees from Payer A.

2. Upon Member 1 authorizing the release of the payment, the front-end platform makes a request to the Queuing Service Back-End affecting the creation of a new payment. The payment is placed in a pending status. Member 1 is responsible for debiting the Payer A DDA account and crediting the Member 1 FAST In-Process account with the appropriate funds required to support the payment.

3. The Queuing Service Back-End identifies this payment as USD to USD and begins processing immediately since there is no currency conversion involved. Processing includes receiving and validating the routing information and preparing the appropriate ledger entries. An “In Network” payment is identified by the originator designating a valid FAST Member unique identifier of the recipient Member (similar to ABA, SWIFT, IBAN, etc., except specific to the FAST program). The Queuing Service Back-End immediately sends a record of the transaction to the FAST Network Central Authority, which will play the role of authoritative check and balance of all transactions within the network. This will be a WORM (write once, ready many) style journal entry, and can assist with investigation of disputes and future reconciliation of transaction.

4. The Queuing Service Back-End notifies Member 2 of a new incoming payment. Notifications can always be found by monitoring the front-end portal, or can optionally be set to email and/or SMS alerts to specially designated Member 2 users, in which case...
alert details can be found within the secured front-end portal. It is now the responsibility of Member 2 to accept the payment, if an auto-accept parameter has not been set.

(5) Payment acceptance is signaled back to the Queuing Service Back-End. A record of the status is immediately sent to the FAST Network Central Authority. The Queuing Service Back-End responds back to Member 2 instructing the credit of 100 USD to their FAST In-Process account.

(6) Member 2 informs Beneficiary A that a payment has arrived.

(7) The Queuing Service Back-End notifies Member 1 of a payment acceptance, instructing Member 1 to debit 100 USD from their FAST In-Process account.

(8) Member 1 informs Payer A with confirmation of successful payment.

**Figure 1c – Domestic Payments Workflow (Out of Network)**

*SCENARIO:* Payer A, an account holder of Member 1 bank, is looking to remit 100 USD to Beneficiary A, an account holder of Non-Member 1 bank. Member 1 is a valid FAST Network Member, however Non-Member 1 is not. Total expected time between Payer A transaction request and Beneficiary A funds availability is 1 day.

(1) The transaction process begins with a request from Payer A to send 100 USD. Payer A interacts with Member 1 to initiate the payment. Member 1 keys the information into the web-based front-end platform. Alternatively, if authorized by Member 1, Payer A may directly enter the payment request into their own customer-facing portal. If known, Member 1 will enter the FAST Member unique identifier of the recipient bank, otherwise the front-end will attempt a lookup of the information to determine whether Non-Member 1 is “in network”, which in this scenario is false. The front-end handles the Member 1 control environment for authorizing payments, its customer disclosures, and guides Member 1 through searching against OFAC prior to release. If desired, the front-end platform also guides Member 1 through assessing and collecting any transaction fees from Payer A.

(2) Upon Member 1 authorizing the release of the payment, the front-end platform makes a request to the Queuing Service Back-End affecting the creation of a new payment. The payment is placed in a pending status. Member 1 is responsible for debiting the Payer A DDA account and crediting the Member 1 sweep account associated with their FedACH operations with the appropriate funds required to support the payment.
(3) The Queuing Service Back-End identifies this payment as USD to USD and begins processing immediately since there is no currency conversion involved. Processing includes receiving and validating the routing information and preparing the appropriate ledger entries. Since Non-Member 1 is not “In Network”, the payment must be routed through traditional mechanisms and will be treated as Same Day ACH. The Queuing Service Back-End immediately sends a record of the transaction to the FAST Network Central Authority.

(4) In the event that no direct integration exists between Member 1 and the Federal Reserve for ACH processing, Member 1 will be able to download a batch NACHA file from the front-end system. Member 1 must process this file within their Fed terminal to originate the payment.

(5) In the event that a direct integration does exist between Member 1 and the Federal Reserve for ACH processing, the Queuing Service Back-End will automatically originate the payment into the Fed system on behalf of Member 1.

(6) The Same Day ACH payment flows naturally through the Fed system as it would today, showing up at the Non-Member 1 institution in the exact same manner as current processing. The Fed system debits 100 USD from Member 1 sweep account, clears the payment, and credits Non-Member 1 with the 100 USD.

(7) Non-Member 1 credits 100 USD to Beneficiary A DDA account, and notifies Beneficiary A that funds have arrived.

Figure 1d – Cross-Border Payments Workflow – Full Match (In Network)

SCENARIO: Payer A, an account holder of Member 1 bank, is looking to remit 100 EUR to Beneficiary A, an account holder of Member 3 bank. Payer B, an account holder of Member 3 bank, is looking to remit 100 USD to Beneficiary B, an account holder of Member 2 bank. Member 1, Member 2, and Member 3 are all valid FAST Network Members. Total expected time between Payer A / Payer B transaction request and Beneficiary A / Beneficiary B funds availability is less than 4 hours. (Please note, the “4 hour” time window is arbitrary and could be extended or compressed based on market volatility. Also, for ease of math in this example, the EUR/USD currency exchange rate will be 1.0000).

(1) [a] The transaction process begins with a request from Payer A to send 100 EUR. Payer A interacts with Member 1 to initiate the payment. Member 1 keys the information into the web-based front-end platform. Alternatively, if authorized by Member 1, Payer A may directly enter the payment request into their own customer-facing portal. If known,
Member 1 will enter the FAST Member unique identifier of the recipient bank, otherwise the front-end will attempt a lookup of the information to determine whether Member 3 is “in network”, which in this scenario is true. The front-end handles the Member 1 control environment for authorizing payments, its customer disclosures, and guides Member 1 through searching against OFAC prior to release. If desired, the front-end platform also guides Member 1 through assessing and collecting any currency exchange spreads and/or transaction fees from Payer A. The estimated currency rate is disclosed to Payer A prior to agreement of the transaction.

[b] Similarly, within a four hour time window of Payer A’s request, Payer B requests to send 100 USD.

(2) [a] Upon Member 1 authorizing the release of the payment, the front-end platform makes a request to the Queuing Service Back-End affecting the creation of a new payment. The payment is placed in a pending status. Member 1 is responsible for debiting the Payer A DDA account and crediting the Member 1 FAST In-Process account with the appropriate funds required to support the payment.

[b] Member 3 handles Payer B in a similar fashion.

(3) The Queuing Service Back-End identifies two transactions in the queue, a payment for USD against EUR and a second payment for EUR against USD. Since there are currency conversion requests within the queue, validating the routing information and preparing the appropriate ledger entries still occurs, however, processing does not begin immediately. The Queuing Service Back-End immediately sends a record of the transaction to the FAST Network Central Authority, which will play the role of authoritative check and balance of all transactions within the network. This will be a WORM (write once, read many) style journal entry, and can assist with investigation of disputes and future reconciliation of transaction.

In currency conversion scenarios, the Queuing Service Back-End will attempt to match inventories of one currency against the offsetting inventories of another. In this case, there is an inventory of 100 USD (that Member 1 has collected from Payer A to support a payment) and an offsetting inventory of 100 EUR (that Member 3 has collected from Payer B to support a payment). And with a EUR/USD effective currency rate of 1.000, it means we have a 100% match. The Solution will keep a 4-hour time window open to promote the collection of more transactions within the matching period. The published currency exchange rate is based off a factor of the market rate at the beginning of any given queue cycle, and in order to calculate matches it is held constant to the Members for the duration of that single cycle.
All matched portions of offsetting inventories will be utilize the Solution as its sole payments mechanism and be transacted quickly and efficiently. Any remaining partial portions must be subsidized by brokering on the open market to ensure the timely remittance of the payment.

To mitigate currency risk there is a subsequent rate monitoring process in place that will automatically close the queue window early and restart the next 4-hour queue cycle should the market rate start moving against the Member and cross a threshold. In that case the window will be closed immediately and transactions will be processed in the same manner as if the window closed naturally. A new set of current exchange rates are in place at the beginning of this current cycle.

At the end of the queue cycle all transactions in the queue are tallied and an assessment of each currency demand is performed. All portions that can be paired off and matched are done so.

(4) [a] The Queuing Service Back-End notifies Member 3 of a new incoming payment. Notifications can always be found by monitoring the front-end portal, or can optionally be set to email and/or SMS alerts to specially designated Member 3 users, in which case alert details can be found within the secured front-end portal. It is now the responsibility of Member 3 to accept the payment, if an auto-accept parameter has not been set.


(5) [a] Payment acceptance is signaled back to the Queuing Service Back-End. A record of the status is immediately sent to the FAST Network Central Authority. The Queuing Service Back-End responds back to Member 3 instructing the credit of 100 EUR to their FAST In-Process account.

[b] The Queuing Service Back-End responds back to Member 2 instructing the credit of 100 USD to their FAST In-Process account.

(6) [a] Member 3 informs Beneficiary A that a payment has arrived.

[b] Member 2 informs Beneficiary B that a payment has arrived.

(7) [a] The Queuing Service Back-End notifies Member 1 of a payment acceptance, instructing Member 1 to debit 100 USD from their FAST In-Process account.

[b] The Queuing Service Bank-End notifies Member 3 of a payment acceptance, instructing Member 3 to debit 100 EUR from their FAST In-Process account.
(8) [a] Member 1 informs Payer A with confirmation of successful payment.
[b] Member 3 informs Payer B with confirmation of successful payment.

Figure 1e – Cross-Border Payments Workflow – Partial Match (In Network)

SCENARIO: Payer A, an account holder of Member 1 bank, is looking to remit 100 EUR to Beneficiary A, an account holder of Member 3 bank. Both Member 1 and Member 2 are valid FAST Network Members. Total expected time between Payer A transaction request and Beneficiary A funds availability is less than 1 days. (For ease of math in this example, the EUR/USD currency exchange rate will be 1.0000).

(1) The transaction process begins with a request from Payer A to send 100 EUR. Payer A interacts with Member 1 to initiate the payment. Member 1 keys the information into the web-based front-end platform. Alternatively, if authorized by Member 1, Payer A may directly enter the payment request into their own customer-facing portal. If known, Member 1 will enter the FAST Member unique identifier of the recipient bank, otherwise the front-end will attempt a lookup of the information to determine whether Member 3 is “in network”, which in this scenario is true. The front-end handles the Member 1 control environment for authorizing payments, its customer disclosures, and guides Member 1 through searching against OFAC prior to release. If desired, the front-end platform also guides Member 1 through assessing and collecting any currency exchange spreads and/or transaction fees from Payer A. The estimated currency rate is disclosed to Payer A prior to agreement of the transaction.

(2) Upon Member 1 authorizing the release of the payment, the front-end platform makes a request to the Queuing Service Back-End affecting the creation of a new payment. The payment is placed in a pending status. Member 1 is responsible for debiting the Payer A DDA account and crediting the Member 1 FAST In-Process account with the appropriate funds required to support the payment.

(3) The Queuing Service Back-End identifies one transaction in the queue, a payment for EUR against USD. Since there are currency conversion requests within the queue, validating the routing information and preparing the appropriate ledger entries still occurs, however, processing does not begin immediately. The Queuing Service Back-End immediately sends a record of the transaction to the FAST Network Central Authority, which will play the role of authoritative check and balance of all transactions.
within the network. This will be a WORM (write once, ready many) style journal entry, and can assist with investigation of disputes and future reconciliation of transaction.

In currency conversion scenarios, the Queuing Service Back-End will attempt to match inventories of one currency against the offsetting inventories of another. In this case, there is an inventory of 100 USD (that Member 1 has collected from Payer A to support a payment) and no inventory of EUR. With a EUR/USD effective currency rate of 1.000, it means we have a 0% match. The Solution will keep a 4-hour time window open to promote the collection of more transactions within the matching period, however in this scenario there are no more transactions within this time window.

At the end of the queue cycle all transactions in the queue are tallied and an assessment of each currency demand is performed. All portions that can be paired off and matched are done so.

(4) Awareness of the upcoming transaction, currently pending, is forwarded to Member 3.

(5) The FAST Network Central Authority acts as a backstop for currency transactions that need to be brokered on the open market, and as such has relationships with foreign exchange providers. When the system has a partial payment amount that must be brokered, the Queuing Service Back-End signals a debit of 100 USD from Member 1 and credits 100 USD to the FAST Network Central Authority.

(6) The FAST Network Central Authority opens a position to buy 100 EUR with the appropriate FX provider for a TOD transaction (same day “today” forward contract) backed by the 100 USD pulled from the Member 1 account.

(7) Delivery instructions sent with the currency order will settle same day and are payment will be delivered to Member 3 for the credit of Beneficiary A.

(8) Member 3 informs Beneficiary A that a payment has arrived.
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>----------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.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>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 sub-sections 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).

Implementation will be phased in over an extended time period to adequately test. An important safeguard is the ability for this Solution to be run in parallel to all pre-existing real world payment systems.

The project lifecycle will consist of the following phases:

- **Phase 1a** – Establishment of FAST Network Central Authority (9 – 12 mon)
- **Phase 1b** – Development of Software and Platform (9 – 12 mon)
- **Phase 2a** – Security and Control Environment Evaluation (6 mon)
- **Phase 2b** – Test Pilot with Small Subset of Early Adopters (6 mon)
- **Phase 3** – Live Pilot with Small Subset of Early Adopters (6 mon)
- **Phase 4** – Aggressive Growth Plan (Ongoing)

Detailed description of each phase breakout:

- **Phase 1a** – Establishment of FAST Network Central Authority
  - (Can be performed at same time as Phase 1b)
  - Official formation of entity
    - Must be a bank or direct partner with a bank (i.e. Federal Reserve Bank) to maintain banking accounts and relationships required to support the platform.
Establishment of relationships with FX provider(s) to facilitate certain aspects of cross-border payments facilitation.

- Establishment of legal paperwork, contracts, compliance hurdles, legal authorities, and operating agreements.
- Establishment of bank marketing strategy and adoption planning.
- Formal authorization of WCUSA as technology support vendor for FAST Network Central Authority.
- Identification of possible bank “early adopters” willing to pilot the FAST payments network in parallel with their existing systems either internally or to a small subset of their customer base.
- Establishment of investigations process and procedures.
- Establishment of long term growth plan for U.S. and international adoption.

**Phase 1b – Development of Software and Systems**

- Determine datacenter plan for housing of FAST hardware and networking systems.
- Buildout of payment transmission messaging format specifications.
- Refactoring of existing WCUSA front-end platform to meet specification requirements.
- Refactoring of existing WCUSA customer-facing front-end platform to meet specification requirements.
- Buildout of queuing and matching infrastructure for cross-border transactions.
- Buildout of integration with FX Providers.
- Buildout of integration with Federal Reserve Network.
- Creation of all necessary documentation and specifications.

**Phase 2a – Security and Control Environment Evaluation**

- Penetration testing.
- SSAE 16 certification.
- Creation of all necessary user and administrative documentation.

**Phase 2b – Test Pilot with Small Subset of Early Adopters**

- Simulated environment for processing real world transactions, but with fake/test data only.
- User acceptance testing from FAST and WCUSA.
- User feedback from early adopter Members accessing the platform.

**Phase 3 – Live Pilot with Small Subset of Early Adopters**

- Extend test pilot activities, however, switch to live transaction processing.

**Phase 4 – Aggressive Growth Plan**

- Implement long-term growth strategy identified within Phase 1a.
Aggressively market and approach banks.

2. 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).

This Solution treats every payment in the same manner, as such, all of the following value propositions are consistent for each use case involved (B2B, B2P, P2B, P2P).

Stakeholders:
- **Payer** (business or individual originating a payment)
  - **Initiation**
    - Payment instructions become intuitive and predictable.
    - Payer has ability to initiate both domestic and cross-border payments via the same predictable mechanism and process.
    - Efficient payments workflow provides opportunity for extremely low cost basis on both domestic and cross-border transactions.
  - **Authentication**
    - Industry standard web-based authentication to protect and encrypt accounts.
    - Ability for Payer to turn on enhanced multi-factor authentication schemes if desire additional security.
    - Ability for Payer to enable email and/or SMS based security alerts if desire additional awareness.
  - **Payer Authorization**
    - Customer-facing front end platform allows Payer to conveniently enter payee and transaction origination requests for themselves.
Cross-border payment experience is enhanced over current FedGlobal offering because Payer will see currency exchange rate prior to approving transaction.

Payer receives a pre-payment disclosure providing visibility of all transaction details and applicable fee structures on both domestic and cross-border transactions prior to approving transaction.

- **Approval by the Payer’s Provider**
  - Real-time status updates on where Payer’s provider is in the transaction lifecycle.

- **Clearing**
  - Easy settlement with Member by maintaining good funds within their DDA account.

- **Receipt**
  - Real-time status updates and near-instantaneous payment receipt via secured web-based front-end.
  - If desired, summary notification of receipt can be sent to Payer via email and/or SMS notification.

- **Settlement**
  - Settlement risk is reduced due to the near instant nature of the process, with no lag between originator and beneficiary and a central register of transaction information acting as the primary repository.
  - Payer is updated of status notifications and has ability to instantly recognize fraud.

- **Reconciliation**
  - The Payer can easily reconcile their bank statement against the Solution’s centralized transaction register via the customer-facing front-end portal.

**Beneficiary** (business or individual receiving a payment)

- **Initiation**
  - N/A

- **Authentication**
  - N/A

- **Payer Authorization**
  - N/A

- **Approval by the Payer’s Provider**
  - N/A

- **Clearing**
  - N/A

- **Receipt**
  - N/A

- **Settlement**
  - Near instantaneous notification of funds received.
- Near instantaneous availability of funds.
  - **Reconciliation**
  - N/A

- **Member**
  - **Initiation**
    - No membership fees to join as a FAST Member or have access to the FAST Network.
    - Easy signup and vetting process for duly regulated banks.
    - This Solution is a unified payments platform that treats all payment origination types singularly and equally (i.e. do not need to know or understand difference between ACH, Wire, SWIFT, etc.).
    - Member can offer the Payer lower transaction fees on similar settlement dated transactions due to platform efficiencies.
    - Member can market and offer the Payer faster payment times across the board.
  - **Authentication**
    - Industry standard web-based authentication to protect and encrypt accounts.
    - Ability for Payer to turn on enhanced multi-factor authentication schemes if desire additional security.
    - Ability for Payer to enable email and/or SMS based security alerts if desire additional awareness.
  - **Payer Authorization**
    - Satisfies Dodd Frank / Reg E compliance
    - Customer-facing front end platform allows Payer to conveniently enter payee and transaction origination requests for themselves, reducing the data entry required by Member staff.
  - **Approval by the Payer’s Provider**
    - Member-definable control environment guiding Member through quick approval of incoming transactions.
    - If desired, capability to provide real-time email and/or SMS based notification of incoming transactions that require approval (to specially designated users).
    - Satisfies Dodd Frank / Reg E compliance
    - OFAC screening technology assists Member compliance
  - **Clearing**
    - Ability to assess transaction fees upon the Payer, which may also include spreads on cross-border currency conversions.
    - Ability to support and maintain third-party integrations with core system providers for G/L interaction, allowing instantaneous sweep directly from Payer’s DDA account into the FAST Network In-Process account.
- Solution enables competition by allowing Member to integrate and transact with other payment processors when sufficient “In Network” routes are unavailable.
  - **Receipt**
    - Real-time status updates and near-instantaneous payment receipt via secured web-based front-end.
    - If desired, summary notification of receipt can be sent to Payer via email and/or SMS notification.
  - **Settlement**
    - Settlement risk is reduced due to the near instant nature of the process, with no lag between originator and beneficiary and a central register of transaction information acting as the primary repository.
    - Member is updated of status notifications and has ability to instantly recognize fraud.
  - **Reconciliation**
    - The Member can easily reconcile their FAST Network In-Process account against the Solution’s centralized transaction register via the customer-facing front-end portal.

- **World Currency USA** (technology and support vendor)
  - **Initiation**
    - N/A
  - **Authentication**
    - N/A
  - **Payer Authorization**
    - N/A
  - **Approval by the Payer’s Provider**
    - N/A
  - **Clearing**
    - WCUSA expects to assess the FAST Network Central Authority a per-transaction fee based on volumes originated through the technology platform.
  - **Receipt**
    - N/A
  - **Settlement**
    - N/A
  - **Reconciliation**
    - N/A

- **FAST Network Central Authority**
  - **Initiation**
    - N/A
  - **Authentication**
    - N/A
In Pursuit of a Better Payment System
Faster Payments Task Force

- **Payer Authorization**
  - N/A
- **Approval by the Payer’s Provider**
  - N/A
- **Clearing**
  - The FAST Network Central Authority may assess the Members a per-transaction fee based on volumes originated through the technology platform.
  - Real-time awareness of the volumes and notional amounts of all payments and status, both domestic and foreign, being transacted through the FAST Network.
- **Receipt**
  - N/A
- **Settlement**
  - N/A
- **Reconciliation**
  - N/A
- **Federal Reserve Bank** (traditional ACH/Wire processor)
  - **Initiation**
    - Take advantage of pre-existing and well established Fed initiation procedures and on-boarding processes.
  - **Authentication**
    - Take advantage of pre-existing and well established Fed security and authentication controls.
  - **Payer Authorization**
    - Member front-end platform provides effective authorization and disclosure mechanisms to reduce risk of payment errors.
  - **Approval by the Payer’s Provider**
    - Member front-end platform provides effective control and transaction workflow mechanisms to reduce risk of payment errors.
  - **Clearing**
    - Take advantage of pre-existing and well established Fed clearing and money flow procedures.
  - **Receipt**
    - Take advantage of pre-existing and well established Fed receipt dissemination.
  - **Settlement**
    - Take advantage of pre-existing and well established Fed settlement procedures and sweep account handling.
  - **Reconciliation**
    - Take advantage of pre-existing and well established Fed resources for use in reconciliation activities.
• **FX Providers** (foreign exchange liquidity and settlement third-parties)
  - **Initiation**
    - Take advantage of pre-existing initiation procedures and on-boarding processes with a single entity, the FAST Network Central Authority.
    - Access to aggregated volumes from all Member banks without needing to individually on-board each institution.
  - **Authentication**
    - Take advantage of pre-existing security and authentication controls based on the FX Provider’s infrastructure backbone (FIX, etc.).
  - **Payer Authorization**
    - Member front-end platform provides effective authorization and disclosure mechanisms to reduce risk of payment errors.
  - **Approval by the Payer’s Provider**
    - Member front-end platform provides effective control and transaction workflow mechanisms to reduce risk of payment errors.
  - **Clearing**
    - Ability to capture new foreign exchange volumes that were previously unavailable when transacted via FedGlobal.
    - Ability to earn spread income currency conversions.
  - **Receipt**
    - Take advantage of pre-existing receipt dissemination.
  - **Settlement**
    - Take advantage of pre-existing settlement procedures.
  - **Reconciliation**
    - Take advantage of pre-existing Fed resources for use in reconciliation activities.

3. **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).

Please refer to Figure 2 for an illustration of the web architecture and integration points.

This Solution treats every payment in the same manner, as such, all of the following integration points are consistent for each use case involved (B2B, B2P, P2B, P2P).

Stakeholders:

- **Payer** (business or individual originating a payment)
  - **Initiation**
    - Payer must work with Member to be on-boarded and approved to transact payments (KYC).
    - Payer may have access to a customer-facing web based front-end platform.
  - **Authentication**
    - Payer will be responsible for their own user account credentials to access the customer-facing front-end platform.
  - **Payer Authorization**
    - N/A
  - **Approval by the Payer’s Provider**
    - N/A
  - **Clearing**
    - N/A
  - **Receipt**
    - Payer may access receipt information directly from customer-facing front-end platform.
    - Payer may download CSV extracts of their own relevant transactions directly from customer-facing front-end platform.
  - **Settlement**
    - Payer must have a banking relationship with a Member institution.
  - **Reconciliation**
    - N/A

- **Beneficiary** (business or individual receiving a payment)
  - **Initiation**
    - N/A
  - **Authentication**
    - N/A
  - **Payer Authorization**
- N/A
  - Approval by the Payer’s Provider
    - N/A
  - Clearing
    - N/A
  - Receipt
    - N/A
  - Settlement
    - Beneficiary interacts with their bank to retrieve funds.
  - Reconciliation
    - N/A

- Member
  - Initiation
    - Institution must request membership access with FAST Network via online mechanism prior to becoming a Member.
  - Authentication
    - Member staff authorized by Member to access the platform will be responsible for their own user account credentials to their front-end platform.
  - Payer Authorization
    - N/A
  - Approval by the Payer’s Provider
    - Member may facilitate optional integration point between their internal compliance, disclosure, and/or transaction monitoring software(s) and the WCUSA technology platform to enable automated reporting of data into those systems.
  - Clearing
    - Member must create a dedicated in-process account on their books (referred to as FAST Network In-Process account).
    - Member may facilitate optional integration point between their core systems provider and the WCUSA technology platform to enable automated G/L entry interaction.
    - Member may facilitate optional integration point between the Federal Reserve and the WCUSA technology platform to enable automated origination of traditional Fed ACH and Wire payments.
  - Receipt
    - N/A
  - Settlement
    - N/A
  - Reconciliation
    - Member may facilitate integration point between their core system provider and the WCUSA technology platform to enable automated
reconciliation reporting or workflows, to tie together the centralized register with the accounting entries made against the FAST Network In-Process account.

- **World Currency USA** (technology and support vendor)
  - **Initiation**
    - N/A
  - **Authentication**
    - WCUSA staff authorized to access the platform will be responsible for their own user account credentials to their management platform.
    - WCUSA maintains and supports the front-end and back-end technology platforms.
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.
  - **Payer Authorization**
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.
  - **Approval by the Payer’s Provider**
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.
  - **Clearing**
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.
  - **Receipt**
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.
  - **Settlement**
    - WCUSA maintains connectivity with the FAST Network Central Authority FX provider relationships. Specifics TBD, but likely foreign exchange transactions messages will be sent through FIX protocol via secured PTP VPN tunneling.
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.
  - **Reconciliation**
    - If requested by the Member, WCUSA works with third-parties to enable value added services through the platform.

- **FAST Network Central Authority** (a bank, or direct bank partner)
  - **Initiation**
    - N/A
  - **Authentication**
    - FAST staff authorized to access the platform will be responsible for their own user account credentials to their management platform.
  - **Payer Authorization**
• N/A
• Approval by the Payer’s Provider
  • N/A
• Clearing
  • Real-time access to system summary transaction data and payment status (scrubbed of PII)
• Receipt
  • N/A
• Settlement
  • Real-time access to system summary transaction data and payment status (scrubbed of PII)
  • FAST must create a dedicated in-process account on their books (referred to as FAST Network In-Process account).
• Reconciliation
  • FAST Network Central Authority may facilitate integration point between their core system provider and the WCUSA technology platform to enable automated reconciliation reporting or workflows, to tie together the centralized register with the accounting entries made against the FAST Network In-Process account.

• Federal Reserve Bank (traditional ACH/Wire processor)
  • Initiation
    • N/A
  • Authentication
    • Pre-existing internal processes to accommodate Fedline/FedWeb security controls with Member.
  • Payer Authorization
    • N/A
  • Approval by the Payer’s Provider
    • N/A
  • Clearing
    • Pre-existing internal processes to accommodate Fedline/FedWeb system access and functionality.
    • Pre-existing optional direct connection directly with Member allowing origination of payments on the Member’s behalf.
  • Receipt
    • Pre-existing internal processes to accommodate Fedline/FedWeb system access and functionality.
  • Settlement
    • Pre-existing internal processes to accommodate Fedline/FedWeb system access and functionality.
  • Reconciliation
- Pre-existing internal processes to accommodate Fedline/FedWeb system access and functionality.

- **FX Providers** (foreign exchange liquidity and settlement third-parties)
  - **Initiation**
    - Pre-existing internal processes to accommodate FX provider access and on-boarding activities.
  - **Authentication**
    - Pre-existing internal processes to accommodate FX provider access and on-boarding activities.
  - **Payer Authorization**
    - N/A
  - **Approval by the Payer’s Provider**
    - N/A
  - **Clearing**
    - Pre-existing internal processes to accommodate FX provider clearing activities.
    - Allow direct connection directly with FAST Network Central Authority allowing origination of aggregated foreign exchange transactions on the Member’s behalf.
  - **Receipt**
    - Pre-existing internal processes to accommodate FX provider receipt dissemination procedures.
  - **Settlement**
    - Pre-existing internal processes to accommodate FX provider settlement activities.
  - **Reconciliation**
    - Pre-existing internal processes to accommodate FX provider reconciliation process.
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).

NOTE:  
VE = Very Effective  
E = Effective  
SE = Somewhat Effective  
NE = Not Effective

Proposers should refer to the Effectiveness Criteria for an explanation of what Very Effective, Effective, Somewhat Effective and Not Effective mean for each criterion.
1. 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.

**Self-assessed rating:**

<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 U.1</td>
<td></td>
<td>Accessibility</td>
</tr>
<tr>
<td>Ubiquity U.2</td>
<td></td>
<td>Usability</td>
</tr>
<tr>
<td>Ubiquity U.3</td>
<td></td>
<td>Predictability</td>
</tr>
<tr>
<td>Ubiquity U.4</td>
<td></td>
<td>Contextual data capability</td>
</tr>
<tr>
<td>Ubiquity U.5</td>
<td></td>
<td>Cross-border functionality</td>
</tr>
<tr>
<td>Ubiquity U.6</td>
<td></td>
<td>Applicability to multiple use cases</td>
</tr>
</tbody>
</table>

**Justification for U.1:**

- **U.1.1 – [SE]** The Solution fully facilitates payments to/from U.S. based banks, however, regulated non-bank account providers would be able to participate through a banking relationship.
- **U.1.2 – [VE]** The Solution provides strong real-time logging reporting of the payment lifecycle, including acknowledgement of funds on the receiving end.
- **U.1.3 – [VE]** The Solution is specifically designed to integrate cross-border payment ability alongside with domestic in a single simplified approach.
- **U.1.4 – [NE]** The Solution does not address the needs of the un-banked.
- **U.1.5 – [E]** The Solution calls for a phased implementation, including an initial pilot followed by an aggressive growth plan.
- **U.1.6 – [VE]** The Solution is designed to integrate with multiple operators.
Justification for U.2:

- **U.2.1** – [E] The Solution provides the capability for a person to access the platform directly via web-based technology, but also offline through direct interaction with their Member bank (phone, fax, in-person, etc.).
- **U.2.2** – [VE] From a technical perspective the minimum amount of information that is required from a Member for a domestic payment is the receiving Member’s FAST unique identifier and the receiving Payee’s DDA account number. To satisfy compliance demands we must also ask for purpose of transaction and name/address information. Additional pieces of information may be requested, such as email and/or phone for optional notification purposes, or additional routing information if the payment cannot be sent via the FAST Network.
- **U.2.3** – [E] The Solution itself is operational 24x7x365, but may be constrained by Members or other third-party relationships.
- **U.2.4** – [VE] The Solution is easy to use, and intuitive to understand for both foreign and domestic payments.

Justification for U.3:

- **U.3.1** – [VE] The Solution is designed as a unified payments system, allowing specific Members to turn off features that they may not wish to take advantage of, but all core features are available to all Members.
- **U.3.2** – [VE] The Solution fully supports disclosures, risk management workflows, exports and reporting, and addresses Dodd Frank / Reg E compliance particular to consumer protection laws governing electronic payment transfers.
- **U.3.3** – [VE] The Solution is based on traditional open non-proprietary web service based standards and verbs utilizing commonly accessible and widely known development approaches.
- **U.3.4** – [VE] The Solution’s core functions remain the same regardless of the input or output channel or medium (i.e. regardless of End User’s choice of channel).
- **U.3.5** – [VE] The Solution provides for specific spots where disclosure language can be added and subsequently displayed to Payers prior to their authorization of the payment.
- **U.3.6** – [VE] The Solution is specifically designed to make all forms of payments commonly understood by creating a unified payments platform that treats all payment origination types singularly and equally (i.e. end users do not need to know or understand difference between ACH, Wire, SWIFT, etc. since all are treated as Payments).

Justification for U.4:

- **U.4.1** – [E] The trade-off of asking for more data is building in complexity and offsetting the “ease of use”, as such in this proposal we erred in favor of enhancing the features of U.2.2. However, the Solution can still be effective in this area, and
messaging standards can certainly be extended to adopt whichever pieces of data are necessary or desired.

- **U.4.2 – [E]** The Solution can immediately support CSV extracts of certain data such as payments and audit log information. The Solution can support integrations with third-party vendors and integrators to provide additional functionality.

- **U.4.3 – [VE]** The Solution will adhere to rigid standards based from the standpoint of providing clear direction and instruction, but as with most web-based API style technologies new major releases will be introduced in the context of versions. Versioning will allow new features to be introduced and adopted (i.e. changing the old standards) without sacrificing flexibility/adaptability over the long term.

**Justification for U.5:**

- **U.5.1 – [VE]** The Solution is specifically designed to integrate cross-border payment ability alongside with domestic in a single simplified approach. Cross-border system will first take advantage of intelligent matching algorithms where currencies will be sourced by other FAST network Members before being sent to the currency exchange market for fulfillment. This is to ensure that all payments will be handled efficiently and timely.

- **U.5.2 – [E]** The Solution is designed to allow foreign banks to become Members of the FAST Network, in which case certain cross-border payments can remain “in network” and at their most efficient. The Solution utilizes large bank foreign exchange liquidity providers to facilitate the currency conversion and payments infrastructure to remit to foreign countries.

- **U.5.3 – [VE]** The Solution is designed to disclose the currency rate of exchange and any local fees to the end user prior to their authorization of the payment. If known, other foreign taxes and fees will be automatically disclosed as well on the Pre-Payment Disclosure form.

- **U.5.4 – [VE]** The Solution facilitates the direct conversion of currency, it does not simply forward USD to the foreign receiver and force the conversion activity on the foreign bank.

- **U.5.5 – [VE]** The Solution already has cross-border elements to the Proposal.

**Justification for U.6:**

- **U.6.1 – [VE]** Solution is a unified full stack front-end and back-end payments platform to allow for the secure inter-connection of the world’s banking institutions in order to provide a single mechanism for money movement. The Solution effectively handles all suggested use case scenarios (B2B, B2P, P2B, and P2P).

### 2. 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.

**Self-assessed rating:**

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

**Justification for E.1:**

- **E.1.1 – [VE]** The Solution allows the Member to add in their choice of providers, and the Solution will determine the most efficient route for the payment at time of transaction.
- **E.1.2 – [E]** The Solution allows the Member to switch among providers and use multiple provides, however the system will need to initially support the third-party provider. As such, there may be a development effort involved to bring that provider online with the Solution.
- **E.1.3 – [SE]** The Solution, per se, would not be involved with the Member’s selection or on-boarding process of their third-party provider. Though somewhat effective from the standpoint that it does not inhibit this from occurring.
- **E.1.4 – [VE]** There is no inhibiting factor to the use of a new third-party other than the technical capabilities of both parties interacting and an evaluation of conformance with the Solution prior to live processing.
Justification for E.2:

- E.2.1 – [VE] The Solution is open to custom integration workflows, and at the base level can support SOAP/XML based web services, RESTful based web services, and FIX Engine connectivity.
- E.2.2 – [VE] There is no inhibiting factor to the use of a new third-party other than the technical capabilities of both parties interacting and an evaluation of conformance with the Solution prior to live processing.
- E.2.3 – [VE] This can easily be part of the contractual requirements imposed by the FAST Network Central Authority as a condition for Membership.

Justification for E.3:

- E.3.1 – [VE] Implementation will be smartly phased in over an extended time period achieving implementation by 2018 and ubiquity by 2020.

Justification for E.4:

- E.4.1 – [VE] The Solution implements a least cost routing approach, with the preferred route as in-network payments. In order to ensure full coverage, the Solution must fallback to support existing payments messaging standards. The Solution will initially support NACHA for domestic and FIX for currency exchange conversions.
- E.4.3 – [VE] The use of the FAST formatting standard is expected to be free to use.
- E.4.4 – [VE] Versioning will allow new features to be introduced and adopted (i.e. changing the old standards) without sacrificing flexibility/adaptability over the long term.
- E.4.5 – [SE] The FAST formatting standard will be transparent, but will be created by both WCUSA and the FAST Network Central Authority which are not standards development organizations.

Justification for E.5:

- E.5.1 – [VE] The Solution comprehensively covers all eight stages of the lifecycle.
- E.5.2 – [VE] The Solution design handles all features, and the securing and scaling of those features.

Justification for E.6:

- E.6.2 – [E] The technical design addresses how the Solution will be architected to allow for scalability.
• E.6.3 – [E] The Solution will be custom software built for the FAST Network Central Authority, and therefore customizable and adaptable to the needs of the changing times.

Justification for E.7:
• E.7.1 – [VE] All Members have access to view their own centralized transaction register, including payment status information. If a suspected error is found, the Member will initiate an investigation with the FAST Network Central Authority.
• E.7.2 – [E] The FAST Network Central Authority will keep records. Future versions of the Solution can certainly provide for enhanced case management tools to enhance the investigation process.
• E.7.3 – [SE] Investigations analysis process and procedures will be established in Phase 1a of the implementation timeline.

3. 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.

Self-assessed rating:

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

**Justification for S.1:**

- **S.1.1 – [E]** The Solution is a living platform with technical and operational resources dedicated to it. As new laws and regulations arise they must be triaged and handled.
- **Solution** offers Member a control environment, including approval authorizations and thresholds, dual authorization, and separation of duties to significantly manage risks.
- **S.1.2 – [VE]** The Solution mitigates risks in the settlement approach by providing real-time access to payment status, centralized (instant) recording of authoritative transaction data, and that same centralized system providing the debit and credit instructions to the Members.
- **S.1.3 – [E]** The technology and support areas of WCUSA will undergo regular third-party assessment of their operational and technical control environment, and satisfactorily maintain SSAE 16 certification.
- **S.1.4 – [SE]** The Solution provides awareness to all relevant parties of transaction and status information for review by the Members to catch fraudulent and/or erroneous payments.
- **S.1.5 – [SE]** The FAST Network Central Authority has the ability to set and impose these items within their Member agreement contracts.
- **S.1.6 – [VE]** The technology and support areas of WCUSA will undergo regular third-party assessment of their operational and technical control environment, and satisfactorily maintain SSAE 16 certification.
Justification for S.2:

- S.2.1 – [VE] The Solution always requires the Payer to authorize their depository institution.
- S.2.2 – N/A – The Solution does not allow pre-authorization.
- S.2.3 – N/A – The Solution does not allow pre-authorization.

Justification for S.3:

- S.3.1 – [VE] The Solution requires the Payer’s depository institution to approve each payment.
- S.3.2 – [VE] The Solution provides the ability for the Member to disclose the irreversibility of the payment to the Payer.
- S.3.3 – [E] The Solution provides the ability for the Member to disclose all relevant consumer protection information to the Payer, including the Payer’s rights in the event that the payment is disputed.

Justification for S.4:

- S.4.1 – [VE] The Solution provides for each Member to determine their hours of operation, and each FAST settlement process is consistent across the Member network with the debiting and crediting of the in-process account at the moment funds are accepted by the receiver.
- S.4.2 – [VE] The Solution has a queuing and processing system that tracks market volatility risks and protects the Members against market swings against the committed open position.
- S.4.3 – [E] The Solution keeps authoritative control of the transaction history centralized with the FAST Network Central Authority, which is presumed to be run by the Fed.

Justification for S.5:

- S.5.1 – [E] The Solution provides the ability for the Member to disclose information to the Payer prior to the Payer’s authorization of the payment.
- S.5.2 – [E] The Solution provides the ability for the Member to disclose information to the Payer prior to the Payer’s authorization of the payment.
- S.5.3 – [SE] The Solution treats returns as a payment, however in the opposite direction. The Member is responsible for evaluating whether to remit the funds back to the originator.
- S.5.4 – [SE] These roles will be discussed and defined in Phase 1a of the implementation timeline.
- S.5.5 – [VE] The Solution fully addresses Dodd Frank / Reg E compliance particular to consumer protection laws governing electronic payment transfers.
Justification for S.6:

- **S.6.1** – [SE] The initial Solution has successful transaction monitoring capabilities, however, does not yet have advanced management capabilities embedded within the platform. Members can rely on data extracts and/or third-party integrations to provide these services, and over time can be implemented directly within the platform.
- **S.6.2** – [NE] Members can rely on data extracts and/or third-party integrations to provide these services, and over time can be implemented directly within the platform.
- **S.6.3** – [VE] The Solution supports real-time access of payment data to all relevant parties.
- **S.6.4** – [VE] The information sharing mechanism is primarily a web-based platform with nothing proprietary for the end user to install or maintain.
- **S.6.5** – [VE] The front-end platform provides granular user controls over the various users within the system, splitting out access by individual permission bits allowing for flexibility in designing the end user’s control environment. Dual authorizations and separation of duties on payment transaction operations is natively embedded within the platform.
- **S.6.6** – [VE] The Solution provides for a centralized trusted authoritative repository of transaction information.
- **S.6.7** – [NE] The Solution does not immediately have advanced management capabilities embedded within the platform. Members can rely on data extracts and/or third-party integrations to provide these services, and over time can be implemented directly within the platform.

Justification for S.7:

- **S.7.1** – [SE] The Solution will account for identity verification, access management, data encryption standards, intrusion prevention/detection. Establishment of specific adopted approaches will be performed in Phase 1b of implementation timeline.
- **S.7.2** – [SE] The Solution will account for data retention policies, physical security measures, monitoring and incident response procedures. Establishment of specific adopted approaches will be performed in Phase 1b of implementation timeline.
- **S.7.3** – [SE] The FAST Network Central Authority will provide oversight and management. Establishment of specific adopted approaches will be performed in Phase 1a of implementation timeline.

Justification for S.8:

- **S.8.x** – [SE] The Solution will account for resiliency mechanisms and systems. Establishment of specific adopted approaches will be performed in Phase 1a and Phase 1b of implementation timeline.
**Justification for S.9:**

- **S.9.1** – [VE] The front-end platform enforces granular user based permission sets on all major functions performed within the platform.
- **S.9.2** – [NE] Since the Solution must fallback to utilizing traditional payment methods, there is an expectation that Payer will need to know various pieces of information from Payee, such as account number in order to correctly route the payment.
- **S.9.3** – [NE] Since the Solution must fallback to utilizing traditional payment methods, there is an expectation that Payer will need to know various pieces of information from Payee, such as account number in order to correctly route the payment.

**Justification for S.10:**

- **S.10.1** – [VE] All parties with a connection to the Solution must be properly authenticated. Most interactions are through the secured front-end platform, however third-party providers will have their own dedicated authentication schemes depending on the specific integration required to support the provider.
- **S.10.2** – [VE] The recipient Member must acknowledge to confirm acceptance of the payment before credit instructions are available for their in-process account.
- **S.10.3** – [VE] The authentication schemes will fully align with bank-grade security standards, including password controlled user accounts with multi-factor challenge questions, ability to enhance with device based two-factor authentication (Authy, Google Authenticator) or SMS based two-factor authentication (SMS based OTP verification). Session timeouts, unsuccessful attempt lock-out with reset mechanisms (time based and administrative resets), password complexity requirements and rotation requirements. Authentication parameter controls governed by the Member to allow them to adjust to their security policies.
- **S.10.4** – [SE] Each separate delivery channel (i.e. third party provider) may enforce their own integration approach.
- **S.10.5** – [E] The Solution treats authentication equally and will impose the user to authenticate their session. Sessions will automatically expire due to inactivity, forcing a user to re-authenticate prior to proceeding.
- **S.10.6** – [VE] The authentication process is a compartmentalized function set, allowing for new or variant authentication schemes to be used without disrupting the remainder of the experience. For example, if the Solution needed to introduce a federated login or other single sign-on type of authentication scheme, that could be implemented and provide a handoff to the system that the session has been properly authenticated.

**Justification for S.11:**
- S.11.1 – [VE] Participant FAST Members must be regulated banking institutions, already compelled and audited on security, resiliency, AML/KYC, and customer privacy (GLBA) protocols.
- S.11.2 – [E] The FAST Network Central Authority will be responsible for vetting a new participant prior to granting Member status. The enrollment process is a necessary vetting step to ensure that the proper boiler plate institution information is on file (official name, address, contacts, ABA, SWIFT, etc.), that the institution is a properly regulated entity within its domiciled region, that the institution has been presented and accepted all of the rules, expectations, and instructions of membership, and to ensure that the institution has agreed to be bound to any legal documentation.
- S.11.3 – [E] The FAST Network Central Authority will be responsible for the ongoing upkeep of Member records and status.

4. 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>Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.1</td>
<td>Fast approval</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.2</td>
<td>Fast clearing</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.3</td>
<td>Fast availability of good funds to payee</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.4</td>
<td>Fast settlement among depository institutions and regulated non-bank account providers</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.5</td>
<td>Prompt visibility of payment status</td>
</tr>
</tbody>
</table>
Justification for F.1:

- **F.1 – [VE]** Payment approval is as fast as the Member feels comfortable designing their control environment, and likely is a matter of a few minutes. Under certain circumstances, the Member may opt to have the system auto-book the transaction immediately after the Payer’s authorization of the payment.

Justification for F.2:

- **F.2 – [VE]** Money flow consists of entry changes in a centralized register which behaves as the accounting differentials required by the Members to their in-process account. The messaging is pushed from the originator to the system where it is processed and subsequent accounting messages are recorded and available for appropriate parties. Clearing of all “in network” Members is facilitated through the establishment and use of a FAST Network In-Process clearing account held at each Member location. Similar to a Fed sweep account, this is the gateway account that is debited and credited providing the fast link between the depositor’s bank account and the FAST Network. Payment clearing between two Members can happen near instantly.

Justification for F.3:

- **F.3 – [VE]** After a transaction has completed, the receipt may be retrieved within the secured front-end platform; the receipt is available immediately upon the recipient confirming acceptance of the payment.

Justification for F.4:

- **F.4.1 – [VE]** The Solution has a queuing and processing system that tracks market volatility risks and protects the Members against market swings against the committed open position.
- **F.4.2 – [VE]** The time-zone becomes a factor in the possible matching of in-network currencies (for example, to match USD/JPY you might be facing a noon transaction in New York where it is 1am in Tokyo), however, that does not necessarily affect the payment mechanism. Time zone differences between Payer and Receiver are not very significant to the placing of the payment.
- **F.4.3 – [VE]** The Solution allows the Member to set their own “trading hours” for both domestic and cross-border payments.

Justification for F.5:

- **F.5.1 – [VE]** All Members party to the payment see real-time status updates at each stage of the transaction. The Payer may always ask the receiving Member for this information, or if the receiving Member has allowed the Payer direct access to the customer-facing front end then the Payer can view this information in real-time for themselves.
• **F.5.2 – [VE]** All Members party to the payment see real-time status updates at each stage of the transaction. The Payee may always ask the receiving Member for this information, or if the receiving Member has allowed the Payee direct access to the customer-facing front end then the Payee can view this information in real-time for themselves.

5. **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.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Criteria Name</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>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.2</td>
<td>Payment system rules</td>
<td>X</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.3</td>
<td>Consumer protections</td>
<td>X</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.4</td>
<td>Data privacy</td>
<td>X</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.5</td>
<td>Intellectual property</td>
<td>X</td>
</tr>
</tbody>
</table>

**Justification for L.1:**

- **L.1.1 – [E]** The legal frameworks used are based on existing banking laws surrounding electronic transfers and customer/data privacy. This includes appropriate provisions of the Dodd-Frank Act / CFPB rules on electronic and cross-border transactions, Regulation E, Gramm-Leech-Bliley Act customer privacy protections, BSA/AML/OFAC for monitoring and reporting of illicit and/or suspicious activities.
- **L.1.2 – [E]** Most notably are the deadlines imposed by the CFPB regarding handling consumer protection of cross-border payments. We are currently in a grace period of
many provisions solidifying currently in 2020 which affect foreign currency transactions, including consumer rights to cancel transactions within 30 minutes after they are placed and several other procedural guidelines for disclosing to consumers.

- **L.1.3** – [E] Members are contractually and legally obligated to adhere to the rules. It is up to the Members to honor those rules, and further disclose and enforce valid participation through their customer base.

- **L.1.4** – [SE] The Solution provides embedded technology to evaluate and handle OFAC screening (which may be turned off if the Member chooses to utilize another third-party service of their own choosing, with or without a custom integration in with our platform). Data extracts of payments will provide Members with the ability to satisfy transaction reporting, and other compliance screenings, within their own pre-existing technology systems.

- **L.1.5** – [E] The Solution should not invoke any unique legal provisions other than complying with existing laws surrounding electronic domestic and cross-border payments.

**Justification for L.2:**

- **L.2.1** – [E] All sub-parts of this key feature (authentication, legal responsibility, payment order initiation and authorization, cancellation, delayed and failed payments, finality and settlement, timing, proof documentation, and error resolution) must all be combined and crafted into legal language used in the Member agreement contract, compiled by the FAST Network Central Authority during Phase 1a of the implementation timeline.

- **L.2.2 through L.2.5** – [SE] Similarly, this Solution has not yet thought out these aspects at the present time. Though somewhat effective in that there is no reason that provisions for each of these sub-sections could not be defined and introduced within Phase 1a of the implementation timeline.

**Justification for L.3:**

- **L.3.1 through L.3.3** – [SE] Similarly, this Solution has not yet thought out these aspects at the present time. Though somewhat effective in that there is no reason that provisions for each of these sub-sections could not be defined and introduced within Phase 1a of the implementation timeline.

**Justification for L.4:**

- **L.4.1 through L.4.5** – [SE] Similarly, this Solution has not yet thought out these aspects at the present time. Though somewhat effective in that there is no reason that provisions for each of these sub-sections could not be defined and introduced within Phase 1a of the implementation timeline.
Justification for L.5:

- **L.5.1 – [VE] –**
  - The Federal Reserve System (FRS) has not in any way committed to provide the services to the proposer, WCUSA.
  - The FX Provider(s) referenced within this Proposal have not in any way committed to provide services to the proposer and/or the FAST Network.
  - WCUSA owns certain intellectual property rights to technology and business methods used throughout this Proposal:
    - All references to the design, features, and technology of the web based front-end platform is based on the existing WCUSA “FXStudio” product and platform (both front-end and back-end).
    - All references to the design, features, and technology of the web based customer-facing front-end platform is based on the existing WCUSA “FXCenter” product and platform (both front-end and back-end).
  - Michael Ruccolo, CEO of WCUSA and member of the FPTF, owns intellectual property rights to business methods used throughout this Proposal. All references to business methods filed within the following issued patents are protected property:
    - U.S. Patent #8,121,923 (https://www.google.com/patents/US8121923)
    - U.S. Patent #8,301,533 (https://www.google.com/patents/US8301533)

6. Governance

Provide a self-assessed rating in the table below and then describe how the solution meets criteria for: effective governance and inclusive governance.

**Self-assessed rating:**

<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>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>
Justification for G.1:

- **G.1.1** – [VE] A FAST Network Central Authority will oversee the Solution, including vetting of Members and the authoritative control mechanism over enforcing the Member rules of engagement. It is a dedicated legal entity created to provide governance, oversight, and limited clearing support to the FAST Membership.
- **G.1.2** – [VE] The governance structure will be transparent and publicly disclosed.
- **G.1.3** – [E] The FAST Network Central Authority should be comprised of several interests, not a single interest. It is recommended that the Central Authority be representatives of various central banks and/or other banking institutions to promote comfort with adoption, especially in foreign countries that may be skeptical of a solely U.S.-controlled platform. Appeals to the system should be brought to the central authority (through a defined procedure to be developed during Phase 1a of the implementation timeline).
- **G.1.4** – [VE] The FAST Network Central Authority will provide for independent validation and assessment of its operations and arrangements.

Justification for G.2:

- **G.2.x** – [SE] The Solution does not currently define these aspects, however, somewhat effective in that there is no reason that provisions for each of these sub-sections could not be defined and introduced within Phase 1a of the implementation timeline.

Appendix A – Workflow Illustrations

Please see attached documents labeled:

- **Figure 1a** – Use Case Stakeholders
- **Figure 1b** – Domestic Payments Workflow (In Network)
- **Figure 1c** – Domestic Payments Workflow (Out of Network)
- **Figure 1d** – Cross-Border Payments Workflow – Full Match (In Network)
- **Figure 1e** – Cross-Border Payments Workflow – Partial Match (In Network)
Figure 1a – Use Case Stakeholders

1. Member 1 (USD)
2. Member 2 (USD)
3. Member 3 (EUR)
4. Non-Member 1 (USD)
5. Non-Member 2 (EUR)
6. Queuing Service Back-End
7. FAST Network Central Authority (Federal Reserve)
8. FedACH
9. FX Prov #1
   - FX Prov #2
   - FX Prov #n

CONFIDENTIAL INFORMATION
Figure 1b – Domestic Payments Workflow (In Network)

1. Payer A initiates the payment to Member 1 (USD).
2. Member 1 sends a payment request to the Queuing Service Back-End.
3. Queuing Service Back-End processes the payment request.
4. Queuing Service Back-End requests a payment confirmation from Member 2 (USD).
5. Member 2 confirms the payment request.
6. Member 2 initiates the payment to Beneficiary A (USD).
7. Member 1 confirms the payment receipt from the Queuing Service Back-End.
8. Payer A receives confirmation of the payment receipt.

In Network

FAST Network Central Authority (Federal Reserve)
Figure 1c – Domestic Payments Workflow (Out of Network)
Figure 1d – Cross-Border Payments Workflow – Full Match (In Network)

```
(1a) Payer A
    Member 1 (USD)
    Front End
    Queuing Service
    Back-End
    (3)
    Member 2 (USD)
    Front End
    Beneficiary B

(2a) (7a)
(2b) (7b)
(4a) (4b)
(5a) (5b)
(6a) (6b)
(7a)
(8a)
(1b)
(2b)
(6a)
(7b)
(8b)

Beneficiary A
Member 3 (EUR)
Front End
Payer B
```

FAST Network Central Authority
(Federal Reserve)
Figure 1e – Cross-Border Payments Workflow – Partial Match (In Network)
This diagram illustrates a Web Architecture with various layers and components:

**Presentation Layer**
- Customer-Facing Front End
- Front End
- XML Web API
- Intranet/Extranet

**Core Processing**
- QUEUING SERVICE
- BACK-END
- AUTHENTICATION
- MATCHING ENGINE
- REPORTING
- DATABASE ABSTRACTION

**Database Layer**
- Database Cluster
- Replication

**External Services**
- Bank Accounts
- FX Provider(s)
- Customer Debit Cards
- Currency Exchange Marketplace
- Third Party Providers (OFAC, Rates, G/L, etc)

**In-Process Clearing Acct**

**Users**
- Retail End User
- Business End User
- Business Customer
- Internet Banking
- Mobile Apps
- Anything
- Staff User
- End User

**Services**
- Internet Banking
- Mobile Apps
- Anything

**Note:** The diagram is labeled as Figure 2 – Web Architecture.
Faster Payments QIAT

PRELIMINARY ASSESSMENT REPORT

Proposer: World Currency USA, Inc.

APPENDIX A: QUESTIONS FOR PROPOSER

Ubiquity

– U.1.1: Please provide further detail on how Regulated Non-Bank Account Providers will integrate into the Solution.
  □ Non-bank account providers must utilize the FAST system through an In-Network bank relationship. The bank will have the “in-process” account infrastructure required to settle the funds.
  □ The Non-Bank Account Provider will have access to a web-based front end portal, allowing them to view their transaction details and provide all necessary transparency on the payment.

– U.1.5: How are Providers motivated to participate in the Solution? Please elaborate on the business case for banks.
  □ For the Bank Members,
    (a) Faster domestic and foreign payments by utilizing the FAST network
    (b) Instant cross-border payment capabilities with a competitive and robust platform
    (c) Dodd Frank / Reg E compliance
    (d) Centrally manage fee income opportunities and P/L reporting from payments
  □ For the FX Providers,
    (a) Participation offers revenues derived from currency spreads on volume of transaction flows.

– U.2.1: Please provide plans for mobile-specific access.
  □ End user customers of Member institutions may have access to a web-based platform and/or mobile application which will allow these customers to securely view transaction history and real-time status, place new transactions, view/edit payee templates, and retrieve disclosures/receipts. It will be the decision of the Member to authorize this use for their clients.
  □ A RESTful API will be expressed allowing the native mobile applications to communicate with the data platform to retrieve relevant information.
  □ The initial mobile apps will be designed natively for Android and iOS operating systems, as well as a mobile-optimized responsive web portal that can be opened on any device’s web browser.
  □ Native apps will be publicly available within their corresponding App stores for free download, though credentials will be required which will only work if they are connecting through a participating Member.
U.2.2: How could the Solution be adjusted so that it does not require users to exchange account numbers?
- The solution could be enhanced to introduce account masking/mapping. If desired, a random unique character string code could be communicated by the receiver which would identify their customer/account entity information within the system to the payer/originator without divulging the true banking account number.
- This unique code could be set to expire after a single use, or after a period of time.

U.2.3, U.2.4: What are the participation requirements and rules for members? How does the Solution require and enforce 24x7x365 access to the Solution for end-users and usability for varying levels of end user needs?
- On the origination side, the technology platform will accept and begin processing any payment requests at any time of day.
- On the receiving side, once a payment is submitted a notification (i.e. webhook) can be sent to the In-Network RDFI, allowing the RDFI to execute a secure API request to pull in the payment details and allow the immediate processing of account entries to the end customer. This provides the ability for automated confirmation receipts and instant crediting to a customer’s account without human intervention.
- We are currently uncertain whether to require a member bank to conform with the 24x7x365 access rules. FAST provides the ability for the Member to be able to support this level, however contractually forcing this may significantly inhibit adoption of the program. Our thought process is to set an adoption time frame, where Members have a grace period while they work towards allowing 24x7x365.

U.3.3: What standard communication and messaging protocols will be used between the Solution and members and between members and end-users? If the payment messaging standards are proprietary (see page 20 in proposal), how will the Solution facilitate a consistent user experience?
- The preferred method of communication between parties is via the web-based portal. FAST is designed to deliver a consistent user experience through its GUI.
- For lower level access to the platform, FAST plans will have a series of RESTful API’s expressed to Members, and plans on supporting the ISO 20022 payments standard allowing Members and end-users to use the APIs to import and export appropriately formatted messages into the platform.

U.3.4: What member rules and guidelines will ensure consistency of experience in offline channels?
- Guidelines and rules for a consistent offline experience are still under development.

U.3.5: Please describe the Solution's error resolution protections, rights, and liabilities
- By default, payments are considered irrevocable at the point of authorized submission into the FAST network. The originating Member is liable for the funds transmitted in all cases.
- It is up to the originating Member to ensure that their In-Process account is properly settled to cover payments made or received via the FAST network.

U.4.1: Please describe the Solution's contextual data capability, providing more detail on the type of contextual data that can be included with payments and the method for doing so. How can "messaging standards be extended to adopt whichever pieces of are necessary or desired" (page 48)? What is the message format used?
All payment messages will have standard data fields, such as sender and receiver information, reason for payment, etc.

Certain use cases may require additional information (i.e. foreign currency transactions to countries with specific document requirements, identification requirements, etc.)

The message format specifics are still being architected, including evaluation of the ISO 20022 usage within the system.

FAST is seeking to adopt the ISO 20022 standard for the payment messaging format. This payment message may be encapsulated within a meta-structure to facilitate efficient communication within the FAST network platform, but all attempts will be made to adhere to the standard and allow external entities to pass and extract relevant ISO 20022 messages.

U.4.2: How does the solution support integrations with business and personal finance systems?

Custom programming for direct integrations would need to be built and maintained by FAST over time, as determined by prioritization of which integration projects will provide the most widespread effect.

Baseline platform capabilities will include CSV download of raw transaction information which may be immediately imported into most external systems.

An API suite will be designed allowing secured access to transactional functions for use of interacting and extracting information into core systems, cash management systems, business and personal finance systems, etc.

U.4.3: How can contextual data be customized in the Solution?

The FAST messaging format will be built to support an extensible set of addendum data records that can be passed along with the payment message, allowing senders and receivers access to the relevant contextual information.

These data records will be open in nature, allowing a sender to pass along virtually any piece of text-based information. These key/value pairings can be used by the sender to tag information of a certain value, and the receiver can key on those user-defined tags.

The system will enforce a prefixed namespace to ensure unique tagging, but this will allow for infinite possibilities of additional information to be embedded and transmitted with the payment without affecting the core remittance information.

U.5.1: Please describe how FAST can expedite its cross-border process. How would this change affect other aspects of the Solution (e.g., currency conversion costs)?

NOSTRO accounts will be held in the name of the FAST Central Authority for each foreign currency that the platform will support. These accounts must be held at in-network Member institutions, and will serve to consolidate all of the inventories across each accepted currency. By utilizing a NOSTRO network, FAST can expedite the payment process by allowing the immediate availability of funds to the foreign counterparty, even before the matching algorithm has determined if and how much currency needs to be purchased from an FX Provider. The NOSTRO accounts make it possible to manage this process, and easily combine matched and non-matched portions of transactions without disrupting the payment to the beneficiary (please refer to new Figure 1f – Cross-Border Payments Workflow diagram attached to these answers).

Availability can be safely made immediately because FAST collateralizes the value of the foreign currency with amount of local currency it has already collected from the originating Member institution.
- This affects the solution by requiring management and oversight of operational accounts. Currency conversion costs were always a factor regardless of this shift, the technology platform guards against shifts in the market volatility ensuring that the cost of the currency does not outpace the rate disclosed to the Payer even over a period of time, thus mitigating the risk to the FAST Central Authority of loss on the FX transaction.

- **U.5.1:** Who determines the FX conversion rate for cross-border payments when the matching algorithm cannot find a match? The FAST Central Authority? Or the provider?
  - The FAST Central Authority will set the rate. This rate will be automatically calculated based on the FX provider’s indication of the market at the moment in time the new rate window is opened, plus a tolerance to compensate for market movement.
  - For example, if the EUR/USD spot rate supplied by the provider is indicated at 1.1000 and the FAST matching window risk threshold is set at 10 basis points, then the rate published to the FAST Member will be 1.1000 + 0.0011 = 1.1011 for EUR/USD payment.

- **U.5.2:** How would the Solution enable transactions with non-member banks abroad?
  - In order to facilitate the payments to non-member banks, we must fallback to a traditional method of international payment delivery for these scenarios in order to ensure delivery.
  - The workflow is very similar to the original Cross-Border Payments Workflow – Partial Match In-Network diagram (Figure 1e), with the notable exception that all funds will be brokered and sent via the FX Provider.

- **U.6:** Please provide more detail on the contextual data capability (U.4 questions)
  - Please see answers to U.4.3 for more information.

**Efficiency**

- **E.1.2:** What steps does the Solution plan to take to make it simpler-yet still secure-for end-users to switch providers?
  - The end user will have the ability to create and manage a centralized user account for themselves which can be used as a single account portable across any FAST Member institutions that they are authorized with.
  - Within the GUI, the end user will be able to seamlessly switch back and forth between Members.

- **E.1.3:** What types of member rules and requirements can FAST put in place to ensure that providers disclose total costs in advance to customers?
  - The web based front-end platform handles all cost disclosure information, applying the “Pre-Payment Disclosure” methodology prior to customer authorization, and “Receipt Disclosure” after the transaction has been executed.
  - The disclosures present the customer information, transaction details (including trade date, available/value date, transfer amounts, transaction fees, exchange rate, transfer tax/fee information when known, third-party fee and other fee information when known, and total amounts), delivery instructions, and free-form disclosure language used to convey bank-specific information and cover consumer protection language (i.e. 30-minute reversal rule, error resolution handling, etc.).
E.2.1: What types of value-added services could Providers offer? How will value-added services be integrated into the common web-based platform? Will Providers be able to create their own interface?

□ FAST Central Authority is agnostic to the specific types of services that could be offered through the platform, so long as the participation requirements are met by the providers ensuring that services are legitimate and useful.

□ Any services that are independent of the core payments operations can be introduced into the platform, but require negotiation and custom integration prior to implementation.

E.3.1: Please provide any further detail on the implementation timeline and growth projections

□ Implementation can be funded from various sources. Either through newly formed FAST Central Authority, or through venture capital routes.

□ WCUSA is currently working on a business plan for adoptability. Associations, core providers, and bank service providers can be incentivized to create awareness of the product.

□ Bank adoption and market share projections are largely influenced by the assumption that the Fed will endorse the platform.

□ Technology timelines are influenced by the fact that there is a portion of the front-end and bank-end platform already in existence.

E.4.1: What is the plan for developing a message format for the Solution? Does the format already exist? What are its characteristics and advantages over existing standards?

□ The format does not already exist, the particulars would still need to be developed.

□ The sole rationale is to develop a standard that is as simplistic and efficient as possible for the FAST network communications, and provide for FAST-specific data fields. Certain meta information and FAST status codes may not be relevant in other standards, it was intended to assist in the direct communication to and from the FAST systems.

□ This FAST format could easily be designed as a wrapper for another settled standard. For example, ISO 20022 XML payment instructions could be encapsulated within the body of the specification.

E.4.1: Why and how would members rapidly adopt and implement the Solution's proprietary messaging standard?

□ Members would rapidly adopt participation within the FAST payment network because of all the business advantages it offers over existing competition. The FAST network comprehensively offers a front- to back- solution, with integration hooks, allowing for the simple and immediate transmission of payments to their beneficiaries. This includes a consistent user experience for transacting both domestic and cross-border payments, while offering advancements in the speed of clearing and notification both to the Members and the end customers. All regulatory compliance is built in within the platform, as well as revenue-generating mechanisms with transaction fee and currency spread handling.

E.4.2: How does the proprietary message format enable cross-border interoperability?

□ Please refer to E.4.1 answer for adoption of ISO 20022 messaging format, which is already widely adopted overseas and would reduce the barrier of entry communicating with the system.
E.4.5: What is the rationale for using a proprietary message format that is not developed or published by a recognized standards development organization?

☐ Please refer to E.4.1 answer for rationale.

E.6: Please provide any further detail on scalability and adaptability

☐ The underlying substructure of message queuing and delivery will employ a low-latency asynchronous bi-directional transport to send and receive message declarations two and from integrations. This may take the form of securing and leveraging the XMPP instant messaging protocol, or other standardized low latency standard, for messaging transport. Technical requirements would adopt a solution that can handily support thousands of concurrent messages per second, and millions of users.

☐ Instructions entered from web- and mobile- based platforms are instantly reflected within the data system and replicated across the infrastructure.

☐ Platform resources will be configured for auto-scaling to adapt to the higher loads at peak times, and reduce resource usage when not peak.

E.7.1: Please describe the exceptions process in detail. What specific tools-e.g., messages, alerts, notifications, and protocols for end-users, providers, and other parties-does FAST provide to address exceptions?

☐ The web-based platform will allow the Member to flag a transaction for either internal review (allowing it to show on an exceptions list within the Member’s system reports) and/or to send an alert to the counterparty Member, assuming that it is an in-network transaction.

☐ As part of the data record, a rolling notepad will be kept allowing both parties to annotate correspondence directly within the data record of the payment.

☐ Email or SMS alerts may be configured by users notifying them of activity.

☐ Contractually, the FAST Central Authority will have the final say in settling a dispute based on a review of the participation guidelines and the findings of the investigation process.

E.7.2: Which transaction records are stored? How long are they kept?

☐ Core information about the payment and routing are recorded for future view of investigators, but any PII will be masked such that the full identity is not revealed. This would allow the record to include dates, rates, amounts, masked account number (described in the U.2.2 answer), country information, masked payer and beneficiary information (truncated to first few letters of name, e.g. “RUCCXXXXXX”), originating and receiving bank information, etc.

☐ All transaction records are stored and archived for future discovery for no shorter than 10 years.

E.7.3: Please describe the design/implementation plan-including the timeline-for aggregating exceptions data to spot patterns at a multi-participant level.

☐ This design/implementation plan still needs to be developed during the implementation phase.

Safety and Security

S.1: Please provide any further detail on the Risk management sub-criteria
The FAST Central Authority will implement a formal Risk Management and Information Security Program to include administrative, technical, and physical safeguards designed to (a) establish measures of acceptable use among internal staff, Member participants, and third-parties, (b) establish a method for assessing and managing risk within FAST, (c) establishing application change, vulnerability, and other controls for information systems, (d) formalize plans for handling business continuity and disaster planning/testing, (e) providing programs and procedures for vendor management, and (f) ensuring proper awareness and handling of all applicable laws and regulations.

Identified primary risks to be managed are: technology risk, capital risk, market volatility risk, settlement risk, credit risk, vendor risk, and reputational risk.

FAST Central Authority will dedicate a Risk Manager role (and supporting team) to continually review, track, and control these primary risk factors.

- S.3.2: When does a payment become irrevocable?
  - The payment becomes irrevocable once it has been authorized by the customer and it is released as a payment to the FAST Network.

- S.3.3: What are the mechanisms and processes in place to protect and compensate the payer in the event of a dispute?
  - By default, the originating Member will be contractually liable for the payment once submitted. In the event of a dispute/investigation process, the originating Member will be responsible for compensating the Payer to the extent of appropriate law and/or customer service decision.

- S.4.1: How does settlement work between the Payer's and Payee's Providers – how does the money move? What are the settlement windows? What existing settlement mechanism is used or what new settlement mechanisms need to be built? Are the "in-process accounts" (page 53) Fed accounts?
  - The “in-process” accounts are not Fed accounts, they are segregated accounts held directly at the Member institution.
  - The system is designed to expedite the settlement process by allowing the banks to control the in- and out- flows of their accounts and not channel funds through an intermediary such as the Fed, unless the specifics of the transaction require it (i.e. payment to a Non-Member institution).
  - Members are responsible for maintaining the correct balances in those accounts, and the FAST technology platform assists with the reconciliation by providing daily settlement summary and detail reports.
  - To further reduce risk in the event of a dispute between two Members, meta-information of each transaction is pushed to the FAST central authority providing a record that can be used to assist in resolving disputes. This can also be used by regulators and internal/external audit to prove the accuracy of the in-process accounts at each Member institution.
  - By default, payments are considered irrevocable at the point of authorized submission into the FAST network. The accounting entry is available for the Member bank instantly upon submission. This allows the bank to settle immediately after the origination.
  - Exact settlement window times are still being established.

- S.4.2: If settlement is not real-time, how does the Solution manage credit and liquidity risk exposures?
The FAST technology platform will provide various safeguards to mitigate these exposure risks, such as measuring net open position exposure (primarily with cross-border related payments), allowing Members to set credit and transaction limits for the customers, and have the system track and alert transaction entries based on these thresholds.

To guard against the credit risk exposure inherent with the Member failing to properly fund their In-Process account at the time of submission, the system will have the ability to query the bank account balance prior to releasing the payment into the network. This query is in the form of direct integration with the bank’s core system.

Further, the originating Member will be contractually obligated with the FAST Central Authority, and is liable for the payment. If an originating Member inappropriately interacts with their In-Process account, the bank will be out of balance on its own books and ledgers.

- S.4.3: Please clarify whether it is settled in central bank money or commercial bank money.
  - Domestic in-network is all commercial bank settlement (please see revised Figure 1b – Domestic Payments Workflow attached to these answers).
  - Domestic out-of-network is a fallback option, in which the Member will have their payment routed through a traditional mechanism such as FedACH, in which case they would settle with the Fed as they do now.
  - All foreign payments will be routed through the FAST Central Authority’s NOSTRO accounts, and settle with FAST to facilitate these payments (please see new Figure 1f – Cross-Border Payments Workflow diagram attached to these answers).

- S.5: Please provide any further detail on the handling disputed payments sub-criteria
  - Processes, procedures, timeframes… The FAST Central Authority will have contract language within the Member participation agreement defining the requirements, processes, and timeframes for unauthorized, fraudulent, erroneous, or otherwise disputed payments or mechanisms. This contract language will hold rule violators responsible by making the decision to limit transaction volume due to risk assessment, and/or suspend or cancel participation based on the findings and frequency of events discovered.
  - It is the responsibility of the Member to comply with consumer protection laws related to disputed payments. The FAST technology platform provides all of the tools required for the Member to comply with consumer error resolution mandates and other consumer protection laws. These tools include providing the ability to customize and deliver consumer-specific disclosure language, tracking the transaction count of consumer payments, and utilizing a pre-payment disclosure to ensure that the consumer has awareness of these regulations prior to their authorization on any payments.
  - An In-Network Payer will have the ability to authorize a reversal/return from within the FAST technology platform. This will in essence originate a separately initiated payment in the reverse direction back to the Payer’s account, which was voluntarily authorized by the Payee.
  - The FAST solution’s approach is still under development seeking consultation with legal consultants.

- S.6.1: Does the Solution require member-banks to share information on fraud?
  - Furthering the capabilities of the FAST platform to expand on information sharing will be developed in the future.

- S.6.2: What is the Solution's intended approach to leveraging data from external entities?
Furthering the capabilities of the FAST platform to expand leveraging data from external entities will be developed in the future.

S.6.3: Please provide the Solution's plan for supplementing its real-time data so that it can support "ex-post management and monitoring of fraud, and provide timely updates and alerts."

Furthering the capabilities of the FAST platform to embed additional aggregation and analysis will be developed in the future.

S.7: Please provide any further detail on the Security controls sub-criteria

Security-related controls, including operational procedures, will be governed by an Information Security Program (please see answer to S.1 for more overview information). This is a bank level risk-based approach to assessing and managing risks, as well as setting prescriptions for the proper way of handling information, systems, and personnel.

Operational procedures and controls will be governed by the Operations Program, detailing the policies and procedures required, on a department by department basis, to conduct approved FAST operations.

Based on the risk assessments performed from the Information Security Program, critical activities – especially with respect heightened risks of insider threats and money movement – should be separated out across separate people, and even separate chains of command where possible.

Information security personnel will oversee the IS operation, including but not limited to monitoring and reviewing the Program policies and procedures to ensure consistency with current requirements and best practices, participating in external third-party assessments and reviews of the control environment and IT/IS standards, performing internal audit functions on critical and non-critical aspects of the FAST platform including reporting findings to the FAST Central Authority managers and governance authorities.

S.8: Please provide any further detail on the Resiliency sub-criteria

Target availability for platform access is 24x7. To achieve this, the FAST architecture must be based on a mesh network of replicated nodes where individual machines or functions can be temporarily pulled out of the meshing for maintenance while not disrupting the operation of live production services. This also requires an operational force in shifts across all hours of the day.

Regular performance monitoring and reporting will provide awareness of target levels. Stress testing will assist in ensuring the consistent durability. Operations and Technical personnel will be tasked with monitoring the systems for potential and eminent issues.

The business contingency planning approach is designed in three phases, (a) incident response, (b) business continuity, and (c) disaster recovery. Incident response is the mechanism where issues are initially reported and triaged (both from the system as well as manually from human input). If incident response process determines that escalation is required, a disaster is declared and business continuity and disaster recovery are triggered. Business continuity ensures the immediate continuity of operations while in the disaster mode, and disaster recovery establishes the long-term cure and recovery of the issue.

A declaration team will be established at the FAST Central Authority, including the establishment of a Disaster Recovery Lead, that are responsible for the execution, testing, and continual review of the business contingency program.
S.9.1: Please describe what the authentication and user based permission sets require from operators and Providers regarding the controls to protect sensitive information

- User authentication is protected by the following:
  (a) Session management – inactive timeout settings, lockout thresholds, IP address whitelist
  (b) Password complexity – time before password expires, minimum password length, character set requirements (numbers, capital letters, special characters)
  (c) Multi-factor authentication scheme – username/password required, challenge questions required, 2FA ability (Authy, Google Authenticator, SMS) if enabled.

- User permissions grant the following:
  (a) Customer functions – view/add/edit/remove customer records, approve customers, override customer fees, view/add/edit/remove payee templates
  (b) Transaction functions – view/add/edit/cancel transaction lists, dual authorization authorities (front and back office), approval authorities (front and back office), view transaction details, process a transaction, view pricing, clear OFAC hits
  (c) Parameter functions – member profile information, view/add/edit/remove branches, view/add/edit/security settings, view/add/edit/remove users and permissions, view audit log
  (d) Report functions – view daily settlement summary and detail reports

S.9.2: If planned, please describe other methods the Solution could adopt for account set-up, transaction set-up, and problem resolution that would not require the use of payers' and payees' account numbers and how these methods would protect sensitive information.

- Please refer to the answer for U.2.2.

S.9.3: If planned, please describe other methods the Solution could adopt for processing and completing payments that would not require the use of payers' and payees' account numbers and how these methods would also protect sensitive information

- Please refer to the answer for U.2.2. By not transmitting the bank account number, you are reducing exposure to customer account information.

S.10.1: Please describe the framework "that operators and providers will use to authenticate providers and end-users to the system."

- Authentication to the web-based management platform is session based. A session is created by the user presenting valid credentials to the system. A unique session token is generated and passed to the user. Each subsequent request will require the presence of the valid token. A valid session must be correctly bound to the initial IP address that was used when the token was generated.

- In order to properly authenticate, the member-bank operator must know their FAST member id along with their username and password. Additionally, at a minimum, a challenge question response is prompted. If enabled, two-factor authentication (Authy, Google Authenticator, SMS) may replace the challenge question prompt.

- If enabled, the member-bank may include a white-list of IP addresses which will ignore any attempts to authenticate from IP addresses not associated with the white list.

- An inactive session will automatically be destroyed after a preset amount of time, forcing the operator to re-authenticate.
S.10.4: How can the Solution enable Members to "apply strong end-user authentication controls across all delivery channels" and are able to "vary the authentication procedure based on the risk-weighting of a given transaction?"

☐ Please refer to answers for S.9.1 for more clarification surrounding authentication methods and capabilities. Authenticated users are governed by user account permissions. Users have the ability for functionality to be turned on and off accordingly.

☐ Certain types of permissions, such as with Member dual-authorization and/or approval permissions, may carry with it levels that may be set based on the risk assessment of the amount of authority the Member requires for the user (i.e. User 1 can place a transaction up to 10,000 USD before requiring dual authorization, or User 2 can approve transactions but only up to 20,000 USD, etc.).

☐ Prior to the release of all payments within the FAST technology platform, the Member user is required to re-authenticate with their password prior to the system submitting the payment.

S.10.5: How will the Solution enable Members to "re-authenticate end-users based on the risk-weighting of a transaction"?

☐ Re-authentication is typically based on user session management monitoring (forced logout, inactivity timeout, etc.). As with S.10.4, all payment transactions will prompt for authentication from the Member user prior to submission.

S.11.1: Please provide more detail on Solution-specific participation requirements that banking regulations do not cover.

☐ The FAST Central Authority will have provisions subjecting the Member to assessment of performance and conformance of FAST rules, regulations, and guidelines.

S.11.3: Please provide more detail about the Solution's processes for monitoring and ensuring providers' compliance with participation requirements

☐ The implementation of regular monitoring still needs to be developed within the implementation phase.

Fast (Speed)

F.1: Please help us understand the rationale for the Very Effective rating in the proposal’s Self-Assessment.

☐ The timeframes described within the proposal also took into account an estimation of non-system human interaction, which is out of the control of FAST and may greatly influence the outcome of the payments timing from the point in time that the end customer first wishes to make the payment until the beneficiary ultimately receives the funds. We included time estimations for the customer to convey the information to the financial institution (or time it may take to key in and review the information for themselves if they are using the mobile application or web-based portal), the time that the member bank may choose to impose additional controls (dual approvals, etc., and the time it may take to clear those approval processes). Additionally, with cross-border payments, the “4-hour” timeframe is a completely arbitrary number and could be set much shorter. Since currency rates shift constantly, the goal of a time window is to allow for the setting of a stable exchange rate within a controlled timeframe to support matching any offsetting currencies. Through patented technology, this time window is controlled and risk of loss is mitigated.
When looking at the time of the payment as of the point of release from the originator to the availability at the receiver, all in-network payments – both domestic and cross-border – have the ability to be approved within the two second expectations.

For in-network domestic transactions, this can vary based on Member-imposed control parameters. The FAST system allows for the Member to set their parameters such that the click of the release button instantly submits the payment information into the FAST network making it irrevocable and instantly communicated to the receiving Member. Conversely, it is possible for the Member to self-impose more internal controls based on their risk posture, which in turn may increase the approval process time. The best example is a dual authorization trigger where the parameters (set by the Member) require a payment that exceeds the specified notional amount to require additional sign-off by a manager.

For in-network cross-border transaction, this is exactly the same consideration as domestic payments.

– F.2: Please help us understand the rationale for the Very Effective rating in the proposal’s Self-Assessment.

Similar to F.1, our timeframes were took into account an estimation of non-system human interaction.

For in-network domestic transactions, the FAST system allows for the capability of settlement within two seconds because at the moment the payment is approved and released into the network a signal will be sent to the receiving Member notifying that a payment has been made (step 4 on our revised Figure 1b – Domestic Payments Workflow In-Network diagram attached to these answers). This notification can be email, SMS, or a custom defined webhook that the Member can set to direct the request to their technology platform. Upon receiving the signal, the Member can make a request to the FAST API to automatically pull in the transaction information (step 5 on our revised Figure 1b – Domestic Payments Workflow In-Network diagram attached to these answers) and immediately process the entries to the customer account. This allows for clearing within seconds because no human intervention is required. The step 5 request to the API also signals the receipt that the receiving Member received the payment which can trigger an instant notification back to the originating Member that the payment was received.

For in-network cross-border transactions, the FAST system behaves similarly to domestic workflow described above, with the exception that there are two independent payments being made – the first is (a) the receiver Member’s FAST In-Process account to (b) the FAST Central Authority’s NOSTRO account of the same currency denomination as the originator Member. The second is from (a) the FAST Central Authority’s NOSTRO account of the same currency denomination as the receiver Member to (b) the receiver Member’s FAST In-Process account. The extra complexity for settlements with the FAST cross-border payments workflow is the notion of matching. (Please refer to new Figure 1f – Cross-Border Payments Workflow diagram attached to these answers).

In order for FAST to instantly authorize the release of foreign payments to the Member prior to spot delivery of the currency into the corresponding NOSTRO account, the FAST Central Authority assumes settlement risk of any amounts brokered on the market through an FX provider. This risk is mitigated by using the value of the local currency it has already collected from the originating Member to collateralize the temporary deficiency of foreign currency it will have remitted from the other NOSTRO account.
F.3: Please help us understand the rationale for the Very Effective rating in the proposal’s Self-Assessment.

☐ Your assessment of a mixed rating is correct. Out-of-network transactions, in all cases, must fallback to a traditional means of remittance mechanism and therefore will carry longer clearing timeframes.

☐ Our answers for F.1 and F.2 should help clarify our VE self-rating for In-network transactions.

F.4: Please refer to questions in S.4 to describe the settlement approach step-by-step

☐ (Please see response to S.4)

F.4.3: Please explain how differences in trading hours or time zones will affect settlement timing as well as credit and liquidity risk exposures

☐ Trading hours and time zones typically affect the availability of human operations personnel. A payment sent at noon in Hong Kong to a U.S. bank would result in needing settlement capabilities at midnight on the east coast. Banks do not typically run 24x7 operations, so therein lies the problem.

☐ The FAST system is designed to allow for automated clearing (described in the answer to F.2 above). When Members are taking advantage of these capabilities, the settlement process for both domestic and cross-border becomes straight-through processing, and the Member can reconcile during the beginning of next business day without affecting the settlement and receipt process to the originator.

☐ To avoid time-zone confusion and normalize the process, the FAST system will record all timestamps in UTC. Regionalized time zones can be calculated from that (i.e. UTC minus 4 hours, UTC minus 5 hours, etc.)

☐ The originating Member contractually assumes a credit risk associated with the payment, irrevocable at the point of submission into the network. The Member must ensure that funds are available from the customer, or accept and maintain the appropriate credit facility with the customer that they are allowing to transact. When the Member authorizes the end customer to transact for themselves (within the web portal or mobile application), the Member defines their own trading hours which will disable the customer from placing transactions during that time period.

F.5: How will World Currency as the Scheme Operator ensure prompt visibility of payment status through operating rules or guidelines?

☐ The FAST platform allows the Member to retrieve real-time status updates, as well as expose all of the real-time status updates to the customer, if they wish.

☐ It is true that the FAST platform places this ability of visibility at the Member institution level, and not necessarily the end-customer. The rationale was to allow the Member institution to know their customer and make the decision for themselves whether to expose that customer to a platform designed to conduct payment transactions.

Legal

L.1.2: Please describe how the Solution will provide consumer protections for cross-border payments.

☐ FAST will option for “real time payment”. Consumer will wave or sign off on their right to 30 minute protection (the statute is still being reviewed to see if consumer may
opt out). Consumer will also have ability to have payment made after 30 minute window.

- L.1.4: How does the Solution support compliance with relevant U.S. law by all end-users and providers when sending and receiving payments? What if complying to US law forces you to breach EU law?
  - U.S. law will take precedence over all transactions.

- L.1.5: How will you impose U.S. rules on non-U.S.-regulated participants?
  - This will be done contractually.

- 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.
  - This area still needs to be developed and will depend if FAST Central Authority is the Federal Reserve or a third party.

- 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.
  - This area still needs to be developed and will depend if FAST Central Authority is the Federal Reserve or a third party.

- L.4: Please provide more details regarding data privacy, including an approach to identify whether and how payment and related information can be collected and disclosed, consistent with applicable policy, law, and End User preference, and an approach, consistent with law, to secure information that should not be disclosed. In doing so, please specifically address how the Solution supports the five data privacy subcriteria.
  - This area still needs to be developed and will depend if FAST Central Authority is the Federal Reserve or a third party.

**Governance**

- G.1.1: Please provide further detail on the Solution's governance arrangement, including policies, structure, and decision- and rule-making procedures.
  - This area still needs to be developed and will depend if FAST Central Authority is the Federal Reserve or a third party.

- G.1.3: Please describe how the Solution plans to handle appeals related to specific decisions or their implementation.
  - This area still needs to be developed and will depend if FAST Central Authority is the Federal Reserve or a third party.

- G.2: Please provide more details regarding inclusive governance, including input and representation from diverse stakeholders, and support for the public interest. In doing so, please specifically address how the Solution supports the five inclusive governance subcriteria.
  - This area still needs to be developed and will depend if FAST Central Authority is the Federal Reserve or a third party.
Figure 1b – Domestic Payments Workflow (In Network)

(Timespan without human intervention between Payer release and Beneficiary availability can be within two seconds)

- **(Step 1)** Payer authorizes payment.
- **(Step 2)** Member 1 credits In-Process account and releases payment to FAST network, payment is irrevocable at this point.
- **(Step 3)** FAST system records payment information with FAST Central Authority, reflecting expected changes to all affected In-Process accounts.
- **(Step 4)** FAST system sends signals of incoming payment to all parties.
- **(Step 5)** Signal automatically triggers query of FAST Queuing Service API for transaction details, allowing Member to instantly credit/debit appropriate accounts.
- **(Step 6)** Upon completion of (5a), Beneficiary is notified by Member 2, or automatically if authorized to directly use web platform and/or mobile app.
- **(Step 7)** Member 1 is signaled with receipt that payment was received by Member 2.
- **(Step 8)** Payer is notified by Member 1, or automatically if authorized to directly use.
Figure 1f – Cross-Border Payments Workflow – Match or Non-Match (In-Network)

(Timespan without human intervention between Payer release and Beneficiary availability can be within two seconds)

- **(Step 1)** Payer authorizes payment.
- **(Step 2)** Member 1 credits In-Process account and releases payment to FAST network, payment is irrevocable at this point.
- **(Step 3)** FAST system records payment information with FAST Central Authority, reflecting expected changes to all affected In-Process accounts.
- **(Step 4)** FAST system sends signals of incoming payment to all parties.
- **(Step 5)** Signal automatically triggers query of FAST Queuing Service API for transaction details, allowing Member to instantly credit/debit appropriate accounts.
- **(Step 6)** Upon completion of (5a), Beneficiary is notified by Member 2, or automatically if authorized to directly use web platform and/or mobile app.
- **(Step 7)** Member 1 is signaled with receipt that payment was received by Member 2.
- **(Step 8)** Payer is notified by Member 1, or automatically if authorized to directly use web platform and/or mobile app.
- **(Step 9)** Un-matched portions are executed with the FX Provider for spot delivery. FAST Central Authority takes open position. (Matched portions of trades already exist in NOSTRO account, and do not need to be brokered).
- **(Step 10)** FAST Network Central Authority remits USD payment to FX Provider to settle EUR currency position.
- **(Step 11)** On spot date, FAST NOSTRO account receives EUR.
Faster Payments QIAT

PRELIMINARY ASSESSMENT REPORT

Proposer: World Currency USA, Inc.

Summary Description of Solution

World Currency USA’s solution, called FAST for the interim, allows contractually bound member-participants (i.e., financial institutions) to connect to each other through a web-based, front-end platform and to clear and settle payments through establishment of FAST in-process clearing accounts located at each member. A separate web-based, front-end platform allows end-users to initiate and view their transactions in real-time.

The FAST solution proposes to consolidate the notion of domestic Automated Clearing House (ACH) and wire payments into a single payment solution for domestic and cross border payments. During its initial stages, FAST would operate in parallel with the existing payment platforms to facilitate adoption and avoid disruption. During this stage, FAST would employ a “least-cost routing” approach for payments. Existing platforms would then be used if they are preferred or if they are the only feasible option (such as when a bank is not a member of FAST).

A FAST Network Central Authority oversees the solution including vetting of members and enforcing member rules. World Currency recommends the Central Authority be comprised of central banks and/or other banking institutions; in places in the proposal (e.g., pg 53) it notes that the FAST Network Central Authority is presumed to be run by the Federal Reserve.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major Strengths
- FAST consolidates payments into a single solution that enables payment through different speeds (e.g., faster payments, ACH, Wire) for both domestic and cross-border transactions
- The solution has the ability to route transactions where available and/or desired through a “least cost routing” approach that uses ACH to reach payees that are not part of the FAST network
- The solution has cross-border functionality that uses an intelligent matching algorithm where currencies will be sourced by other peer network members before being sent to the currency exchange market for fulfillment

■ Areas for Improvement and Enhancement
- The solution proposes to create a new global network, but its advantages over existing networks are not clear and it will be critical to motivate providers to participate and make the solution available to end users
- Because it is bank-centric, FAST is less accessible to non-banks than current offerings. Regulated Non-bank Account Providers can participate through a banking relationship of the solution, but banks need to be motivated to enable non-banks to participate
- The solution allows member-banks to control the end-user’s experience, but more clarity needed on how the solution will require and enforce any base level operating rules to ensure a minimum standard in feature functionality or consistency of user experience for usability and predictability.
- More clarity is required on the settlement approach for how money moves between members (not just information exchanged through clearing)
Use cases addressed

– The solution addresses all use cases—B2B (business to business), B2P (business to person), P2B (person to business), and P2P (person to person)—for both domestic and cross-border payments

Proposer’s overall ability to deliver proposed solution

– The solution is based on hub-and-spoke models used in payment systems today, so the concepts are proven

– Patents have been filed as related to components of the solution, but full technical solution including software and platform is not yet developed

– Implementation plan is high level and needs next level of detail to understand viability
Ubiquity

U.1 Accessibility

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution is accessible to any financial institution (FI) but requires non-banks to gain access through a bank partner (U.1.1). The solution is able to reach all payees with a banking account—either through their member banks or by interoperating with existing payment systems such as same-day ACH (U.1.2). Interoperability with the ACH network is achieved through members originating the payment into the Federal Reserve system in cases where the payee is a customer of a financial institution that is not a member of FAST. The solution also supports multi-currency transactions (U.1.3).

While the proposal states that Regulated Non-Bank Account Providers can access through banking relationships, because users must have a bank account, the solution recognizes that it does not address the needs of the unbanked (U.1.4). Further, more detail would be helpful on how banks would be motivated to provide access to non-banks (U.1.1).

U.2 Usability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution is available 24x7x365 through multiple channels including web, call center, fax, in-person and mobile (U.2.1, U.2.3). However, it is up to members to make FAST available to their end-users; if a member does not provide services 24x7x365, then the FAST solution might not be available 24x7x365 either. An adoption time frame will likely be set up where members have a grace period while working towards 24x7x365.

However, the solution does not enable the initiation of payments with limited payee information, as it requires that the payer know the payee’s checking account number and the receiving bank-member’s FAST identifying number to make a payment (U.2.2). It offers a way to use account masking through a random unique character string code that expires, but more clarity is needed on how an alias could be used to send payments to improve usability for end users.

Moreover, the solution does not provide any requirements or enforcing mechanisms related to accommodating varying levels of end user technological proficiency and usability needs (e.g., disabled, elderly, language) (U.2.4).

U.3 Predictability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution design delivers on the defined baseline of core features and supports the communication of these baseline features to end users (U.3.1-2). It also uses standard, web-
based communication and messaging protocols (U.3.3). The solution is described by the term “FAST” (U.3.6).

However, more detail would be helpful on how the solution will require and enforce a level of predictability for the end user around the experience such as through guidelines or operating rules for providers (U.3.2, U.3.4). Additionally the proposal notes that the originating member is liable for funds transmitted in all cases but more detail is needed on the error resolution, protections, rights, and liabilities of the payer and payee (U.3.5).

### U.4 Contextual data capability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale**

The proposal indicates that the solution will use ISO20022 though also notes message format specifics are being architected (U.4.1). Custom programming will be used for direct integrations with business and personal finance systems, though baseline platform capabilities will include CSV download of rawn transaction information (U.4.2). Standards will be balanced with flexibility through a message format that supports extensible set of addendum data records with a prefixed namespace to ensure unique tagging (U.4.3).

The solution is still architecting and developing its full set of contextual data capabilities and would be enhanced with more details on the design of the contextual data including how the proprietary format referenced for contextual data will be a wrapper for ISO20022 (U.4.1, U.4.3).

### U.5 Cross-border functionality

<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 cross-border payments using a matching algorithm that reduces conversion costs by sourcing currencies from other, peer network members before sending them to the currency exchange market for fulfillment. Nostro accounts held at in-network member institutions in the name of the FAST Central Authority for each foreign currency are used to expedite the payment process by allowing immediate availability of funds even before the matching algorithm has completed (U.5.1). Interoperability with other payment systems will rely on traditional methods of cross border payments with non-FAST banks (U.5.2). The solution requires advance disclosure of fees, exchange rates, and other end-user costs (U.5.3) and enables currency conversion (U.5.4).

The solution embeds some of cross-border functionality into the overall implementation timeline but more detail is needed on how the solution will achieve adoption and ubiquity for cross-border payments (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 can apply to a broad range of use cases, though once contextual data capabilities are designed, there will be a better sense for how applicable the solution will be to business 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 enables competition by allowing members to add their choice of providers (focus of the self-assessment), but also allows end-users to choose any Regulated Non-Bank Account Providers (through a member) or any member as their provider (E.1.1). The solution allows providers regardless of size to become a member as long as participation requirements are met (E.1.4). Providers can make disclosures to end users through the web based front-end platform (E.1.3).

However, more detail would be helpful on how non-banks will be afforded access to the solution through banks (E.1.1). In addition, more clarity is needed on how end users would designate into which provider account they want to receive money and easily switch providers or use multiple providers (E.1.2).

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:
The solution uses open, accessible standards to help its members integrate and offer value-added services (E.2.1). Providers are allowed to provide value added features as long as participation requirements are met (E.2.2). In addition, the solution needs to ensure that members clearly disclose to customers that the value-added services are optional; the proposal mentions that this requirement could be included in the contractual arrangements (E.2.3).

However, the proposal makes limited mention of APIs, and instead, focuses on the web-based platform which would make services essentially identical between providers. This may make it difficult for providers to differentiate and compete, even if price is set by providers. More detail is needed on the potential opportunity for providers to use APIs to design their own interface and differentiate on that basis; and also on the type of messaging/information flow that is planned for the system which would enable differentiating services.

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 solution provides a four phase timeline for implementation over two years that includes:
Phase 1: Establishment of FAST Network Central Authority and Development of the Software and Platform (9-12 months); Phase 2: Security and Control Environment Evaluation and Test Pilot with Early Adopters (6 months); Phase 3: Live Pilot with Early Adopters (6 months); and Phase 4: Aggressive Growth Plan (Ongoing).
This timeline is aggressive based on historical case examples and more details in the implementation plan are needed such as: how the solution’s implementation will be funded (indicates it could be from venture capital or a newly formed entity), the particular entities WCUSA expects to adopt FAST, implementation and ubiquity hurdles that might arise and how WCUSA will overcome those obstacles (e.g., achieving adoption, engaging both domestic and foreign banks), market share and growth projections. While a portion of the technology is already in existence, the business plan for adoptability is in progress.

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:
The proposal states that FAST’s proprietary message format is interoperable with other, standard formats and will enable cross-border interoperability with ISO20022, however the format is under development (E.4.1-2).
As such, more detail is on how ISO20022 will be implemented with the proprietary format (E.4.1), whether the format is as cost-effective as standard formats for members (E.4.3). As a proprietary format, the proposal indicates that the messaging format is not developed or published by a recognized standards development organization (E.4.5).

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 supports every step of the end-to-end payment process, from initiation to reconciliation (E.5.1) in concert with its members. Its technical design supports all of the solution’s 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 solution indicates that its technical requirements would support thousands of concurrent messages per seconds (E.6.1).
However, further detail would be helpful on how the technical design can scale at peak times, the stress tested capacity of the solution (E.6.2), and how it can adapt to ongoing developments (E.6.3).
E.7 Exceptions and investigations process

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution enables members to view their own transactions and to initiate investigations with the FAST Network Central Authority (E.7.1). There is a web-based platform that allows members to flag transactions for review, send alerts and correspond to address exceptions or disputes. The FAST Central Authority has the final say in settling disputes. Members have access to a centralized transaction log to support error resolution and all records are stored for at least 10 years (E.7.2).

Further detail would be helpful on the protocols and timeframes for addressing exceptions (E.7.1). In addition, the solution does not yet aggregate exceptions data to spot patterns across participants, but the proposal indicates the intention to offer this last capability during the implementation phase (E.7.3).

Safety and Security

S.1 Risk management

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The FAST Central Authority will be implementing a formal Risk Management and Information Security Program. The solution will undergo regular third party assessment of operational and technical control environment (S.1.3, S.1.6).

However, the proposal does not define a risk management framework with rules, policies, and procedures to address the risk of an unexpected application of a law or regulation, risks related to settlement, operational risks, unauthorized, fraudulent or erroneous payments, and incentives offered to operators and providers to address and contain the risks they pose to other participants (S.1.1-S.1.6).

S.2 Payer authorization

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution requires payers to authorize each payment to their member-bank at the time of payment initiation (S.2.1). FAST does not have pre-authorization capability (S.2.2-3).

S.3 Payment finality

Very Effective  Effective  Somewhat Effective  Not Effective
Rationale:
The payer’s member-bank approves each payment and assures the availability of good funds (S.3.1). The payment becomes irrevocable once authorized by the payer and released to the FAST Network (S.3.2). The solution gives members the ability to disclose all relevant consumer protection information to the payer when payments are disputed and holds the originating member responsible for compensating the payer.
More detail would be helpful on what happens in a dispute, however, elsewhere in the proposal it is noted that the FAST Central Authority will be the ultimate arbiter of disputes (S.3.3).

S.4 Settlement approach

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
This solution has outlined an approach to settlement that involves “in-process” or segregated accounts held directly at each member institution. The proposal notes that clearing of member is done through the in process account that is debited and credited, and that settlement occurs once the receiving member acknowledges the acceptance of the incoming payment.
However more clarity is needed on how money actually moves – the segregated account held at each member institution can be used to clear funds (debit and credit a ledger) but there will be net receiving institutions with an overhang of funds owed. The solution does not detail how the money will move from one provider to another, and how the settlement risk is managed.

S.5 Handling disputed payments

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution provides the platform and tools required for members to comply with consumer error resolution and consumer protection laws (S.5.2). The platform also enables a payer to request a voluntary return of funds from the payee (S.5.3).
While the solution indicates it will have a participation agreement that defines the requirements, processes, and timeframes for disputed payments or mechanisms, these are under development (S.5.1, S.5.4, S.5.5).

S.6 Fraud information sharing

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution shares real-time information on successfully executed transactions through its web-based platform (S.6.1). It supports differential access to content based on the roles and responsibilities of its operators, providers, and regulators (S.6.5). The FAST central authority stores and aggregates this information (S.6.6).
However, the solution does not yet collect the type of information needed—such as data on rejected transactions—to manage and monitor fraud (S.6.1), and the proposal does not
specifically describe plans to do so in the future. The solution does not require member-banks
and participants to share fraud-related information (S.6.1), nor does it leverage fraud-related
data from other entities to share with operators and providers (S.6.2). FAST does not support
real-time and ex-post management and monitoring of fraud or provide timely updates and alerts
(S.6.3); rather, it “supports real-time access of payment data to all relevant parties” (page 53).
Finally, the solution does not yet aggregate and analyze fraud information to spot patterns
across participants (S.6.7); participants are expected to rely on “data extracts and third-party
integrations” to perform this function themselves (page 54).

S.7 Security controls

| Very Effective | Effective | **Somewhat Effective** | Not Effective |

**Rationale:**
The solution will have an Information Security Program to assess and manage risks and set
policy for information handling and personnel, as well as an Operations program to detail
policies and procedures.

As such, the proposal acknowledges a need for Security Controls and sets out a development
path during the implementation phase, but it is not yet complete. The QIAT has interpreted the
Effectiveness Criteria such that solutions at this stage of development earn a rating of
“Somewhat Effective.”

S.8 Resiliency

| Very Effective | Effective | **Somewhat Effective** | Not Effective |

**Rationale:**
The proposal provides an overview of the approach to Resiliency including a declaration team
established at the FAST Central Authority including the establishment of a Disaster Recovery
Lead to oversee the business contingency program (S.8.4).

As such, the proposal acknowledges a need for Resiliency and sets out a path to complete it
during the implementation phase, but it is not yet complete. The QIAT has interpreted the
Effectiveness Criteria such that solutions at this stage of development earn a rating of
“Somewhat Effective.”

S.9 End-user data protection

| Very Effective | **Effective** | Somewhat Effective | Not Effective |

**Rationale:**
The authentication and user-based permission sets in the front-end FAST platform provide
operators and providers with robust controls and mechanisms to protect sensitive information
(S.9.1).

The solution indicates that sensitive information like account numbers can be protected through
single use codes that provide account masking (S.9.2-S.9.3). While this can support end user
data protection, it is not create a straightforward and simple end user experience.
S.10 End-user/provider authentication

<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 has a robust framework and mechanisms for identification and verification as it enrolls end-users and providers and facilitates transactions (S.10.1). The payee’s provider must communicate acceptance of a payment before finalizing the transaction (S.10.2). These mechanisms and framework align with regulatory guidance and industry standards (S.10.3). End-users are authenticated initially to the solution, and FAST requires providers to re-authenticate end-users when needed (e.g., if the session expires due to inactivity) (S.10.5). Authentication models can also be changed if the threat landscape changes (S.10.6).

The solution itself does not control authentication; members authenticate end-users and select their own authentication controls. More information is therefore needed on how the solution would enforce them. In addition, it is not clear whether authentication and re-authentication can be varied based on risk-weighting or any other factors for all consumer and business transaction types (S.10.4-5).

S.11 Participation requirements

<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 FAST Network Central Authority vets new member-banks before they can become members and maintains member records and status (S.11.1, S.11.2). The Authority will also be responsible for upkeep of member records and status (S.11.3).

The proposal does not address processes to regularly monitor and ensure member compliance with the participant requirements (S.11.3).

Speed (Fast)

F.1 Fast approval

<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 enables approval within 2 seconds for in-network payments, but it allows for the member to set their parameters to self-impose more internal controls based on risk, which would increase the approval process time (e.g., dual authorization). Thus, the operator, provider and operating rules ultimately control the speed of approval.
F.2 Fast clearing

| Very Effective | Effective | Somewhat Effective | Not Effective |

**Rationale:**
The solution enables clearing within 2 seconds for in-network payments, but as above it allows for the member to set their parameters to self-impose more internal controls based on risk, which would increase the approval process time (e.g., dual authorization) and hence the speed of clearing. Thus, the operator, provider and operating rules ultimately control the speed of clearing.

F.3 Fast availability of good funds to payee

| Very Effective | Effective | Somewhat Effective | Not Effective |

**Rationale:**
The solution enables availability of funds within 1 minute for in-network payments, but as above it allows for the member to set their parameters to self-impose more internal controls based on risk, which would increase the approval process time (e.g., dual authorization) and hence the speed of availability of funds. Thus, the operator, provider and operating rules ultimately control the speed of funds availability.

More detail is needed on whether the funds availability for cross-border payments is four hours or a shorter time frame that the proposal indicates is possible.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

| Very Effective | Effective | Somewhat Effective |

**Rationale**
As with S.4, the solution has outlined an approach to settlement that involves “in-process” or segregated accounts held directly at each member institution. The proposal notes that clearing of member is done through the in-process account that is debited and credited, and that settlement occurs once the receiving member acknowledges the acceptance of the incoming payment.

However more clarity is needed on how money actually moves – the segregated account held at each member institution can be used to clear funds (debit and credit a ledger) but the solution needs to detail how the money moves from one provider to another whether through Central Bank money or commercial bank money, and how the settlement risk is managed (F.4.1, F.4.3).

F.5 Prompt visibility of payment status

| Very Effective | Effective | Somewhat Effective | Not Effective |
Rationale:
The solution provides member-banks with “real-time status updates at each stage of the transaction” (page 57), but it is up to each member to determine whether and when the payer and payee have visibility into payment status.

Legal

L.1 Legal framework

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
The solution identifies relevant legal sources (L.1.1) and identifies a gap in covering consumer protections for cross-border payments with a plan to address this gap (L.1.2). Members are contractually and legally obligated to adhere to the solution rules (L.1.3).

However, the proposal does not describe the main components and dimensions of the legal framework. The solution supports legal and regulatory compliance related to OFAC screening (L.1.4) and does not see any unique legal provisions that are needed for situations where parties perform the same function but are subject to different laws or regulations (L.1.5). However, as cross border is a target use case, the solution should consider how it will support compliance with relevant U.S. law by all end-users and providers particularly in cases of conflicting laws. Similarly the solution does not address how it will reconcile U.S. rules with non-U.S. regulated providers in cross-border payments.

L.2 Payment system rules

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
The proposal acknowledges a need for Payment system rules and sets out a path to complete it during the implementation phase, but it is 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

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
The proposal acknowledges a need for Consumer protection and sets out a path to complete it during the implementation phase, but it is 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.4  Data privacy

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The proposal acknowledges a need for Data privacy and sets out a path to complete it during the implementation phase, but it is 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.5  Intellectual property

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution’s approach to intellectual property rights addresses all risks arising from third-party rights related to patents, trademarks, copyrights, and trade secrets. The approach resolves or manages these risks prior to implementation.

Governance

G.1  Effective governance

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution’s governance approach includes public disclosure of governance arrangements (G.1.2) and provisions for independent validation of compliance with the solution’s rules, applicable law, and achievement of objectives (G.1.4).

While the proposal describes a central governance authority, it does not address “efficient decision-making and rule making” or define policies and structure (G.1.1). Because the solution plans to define the appeals process during implementation, the proposal does not include information on the process (G.1.3).

G.2  Inclusive governance

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The proposal acknowledges a need for Inclusive governance and sets out a path to complete it during the implementation phase, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
**APPENDIX A: ASSESSMENT SUMMARY**

- ✓ = QIAT Assessment  
  ○ = Proposer Self-Assessment

### UBIQUITY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

### EFFICIENCY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

### SAFETY AND SECURITY

<table>
<thead>
<tr>
<th>S.1: Risk management</th>
<th>S.2: Payer authorization</th>
<th>S.3: Payment finality</th>
<th>S.4: Settlement approach</th>
<th>S.5: Handling disputed payments</th>
<th>S.6: Fraud information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

Page 14
<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.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

We want to thank you for the time put into our proposal assessment. We acknowledge that there are some areas the “Somewhat Effective” box was checked due to lack of information.

Due to this type of venue and platform for release, we can not provide you with information we believe to be “Confidential Intellectual Property”. If at any time there is further interest to discuss we would be happy to discuss on a one on one basis with proper NDA put into place.
WORLD CURRENCY PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

Please share your concerns about this proposal’s assessment against the Effectiveness Criteria.

Missing modern use of mobile payments. No pre-authorization. No fraud data analysis and information sharing. Using regular passwords as default. Appears to be basically an interbank settlement solution and not a real digital payment solution missing on many of the effectiveness criteria.

Ubiquity assessment ratings unfair. The solution does provide accessibility and usability in that it mirrors ACH and wire routing and methodology.

Efficiency rating does not give credit for the solution’s intent to allow for least cost routing, which would be competitive and meet all users’ needs.

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 does not include the unbanked. The solution does not include pre-authorization capability, yet S.2.1 was rated VE. The solution’s payment formatting is questionable. The solution does not aggregate exception data. The proposal lacks clear risk management, legal and governance frameworks.

Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

Solution is not operational, as Network Central Authority and software do not exist. Rules and governance are not fully described.

I believe the proposal was fairly assessed. I liked how the system operates in parallel with existing platforms though I struggle as to whether financial institutions will join the system as I am not sure I see a true value proposition. I am also unsure as to whether the FED will agree to be the operator and overseer of such a system.
Rules and governance need more details. In attending the question and answer session in person, many answers focused around elements "will be developed," rules, governance, models, and more.

Contextual data capability is rated too highly, as this area is still under design, and not apparent how it will be uniformly, consistently understood and utilized by both senders and receivers. Rules and governance areas are too highly rated, as the specifics are not provided.

I appreciated the QIAT's commentary around implementation and the Proposer's ability to deliver. Our efforts (TF members, Fed staff and QIAT) in assessing the merits of each proposal are wasted if implementation issues mean the proposal will never see the light of day.

Would like more detail on dispute resolution, legal framework and governance.

1) Available 24/7/365, 2) available in multiple channels, 3) enables approval within 2 seconds, 4) FIs can set parameters to self impose greater internal controls based on risk.

I will simply say World Currency USA seems to be open to different methods of payments. Governance and interoperability may take longer as far as timeline but this seems to be on target for a good initiative.

Proposal is too vague in areas of security, legal, and governance criteria, which was noted by the QIAT.

The legal and governance frameworks are works-in-process. I do not agree with the QIAT’s arbitrary assessments in these criteria.

World Currency misses the mark on Governance.

Agree as assessed. Solution proposal is very light on details of key criteria elements.

The proposal is so "conceptual" in nature; hard to truly assess.

I agreed with the assessment especially when it comes to access and to the necessity of creating a new network. Not understanding clearly the added value of duplicating existing rails.

The World Currency USA proposal is not so varied from some of the current interconnect members solutions for banks, given that this solution is bank-centric. Not sure how this solution is markedly different from the current state in which banks interconnect.

Is a “unified full stack front-end & back-end payment solution to allow for the secure inter-connection of the world’s banking institutions in order to provide a single mechanism for the money movement.” The reviewers are also concerned that the payer must know the payee’s checking account information.
TASK FORCE SOLUTION-ENRICHING COMMENTS

Ubiquity

The proposed solution could be enriched by providing a plan for non-financial institutions to offer the FAST payments system. Describing how the FAST payments system would interoperate with other real-time payment systems would also enrich the proposed solution.

Up to the member FIs to make the solution available to their customers.

End-user experience will be Member FIs must fund.

How to engage foreign and domestic banks.

2-year timeline does not seem realistic, proposal did not outline risk management framework and rules.

I struggle with the ability to make the solution work in today's payment world. Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. I am not sure that there is a strong value proposition for service providers and their client FIs to use the product. I would like to see a road map for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium-sized financial institutions.

One of the main questions is that, while this solution is bank focused, how will non-bank involvement occur? This is a question central to ubiquity because it is through non-banks that others will be reached, such as the underbanked or the nonbanked. Without such reach it can't be considered ubiquitous.

Another question is the value proposition. Why would banks participate if they would incur costs but not much would change? They would most likely still transmit the majority of their transactions over the current systems unless the faster payment solution were cost-effective.

Efficiency

The proposed solution could be enriched by providing additional information around payment finality, settlement, dispute resolutions, security controls, and fraud monitoring.

Payer must know the payee’s checking account #.

Unpredictability to add value-added services limited due to API limitations/opportunities.

Provide more details on APIs, how they will be designed and deployed across participants.

Is there an implementation that could be done, independent of FED involvement?

24/7/365 is only achievable if the member FIs make it possible. Currently this is not possible over weekends or holidays. How will the solution force 24/7/365?
More detail on how things can be automated in terms of processing and reconciliation would be helpful. Reading the proposal it seemed there were a lot of manual operations especially with regard to providing disclosures to consumers for cross-border.

**Safety and Security**

The solution could be enriched by providing additional information around payment finality, settlement, dispute resolutions, security controls and fraud monitoring.

Too vague in many of the criteria in this section—needs development.

Solution will not collect data on rejected transactions to manage and monitor fraud. Security controls and Resiliency framework are somewhat effective.

It appears that the solution falls back to traditional payment methods, meaning that the payer will need to know the payee's account number to route payment. This is a far less secure approach than most other proposed solutions, which rely on push payments without any need for the payer to know the payee’s account number.

**Speed (Fast)**

Need to address real-time availability. ACH mimic is good for simplicity but the entire solution is just what we have today. Not faster payment.

Approval speed will vary between FIs based on their ability to set more internal controls due to riskier transactions.

**Legal**

The solution could be enriched by providing the overall network rules and legal framework for the FAST proposed solution.

Not enough details in this area - more clarification/details will strengthen the proposal.

Describe rules in more detail.

I would have liked to see some suggested implementations for a legal, rules, protection, privacy framework.

**Governance**
The solution makes note of a FAST Network Central Authority made up of central banks and/or other participating institutions. However, the solution could be enriched by detailing how central banks within different countries might develop a governance to support the FAST Payments network.

Additional details would strengthen proposal.

The WC proposal raises an important issue regarding interoperability. That is, how critical is the need for faster payments schemes to be interoperable with existing payments systems on Day 1 of launch? WC suggests that it will include ACH and Fed Wire payments options along with its FAST digital currency network solution. No other solutions introduce the same notion. Yet, how does a new scheme propose to be both inclusive and capable of reaching critical mass without having at least a back door option to reach non-scheme participating FIs and their members without having the ability to gateway to other options? Assuming that this form of interoperability is a condition precedent to widespread adoption would assume then, that interoperability governance would need to be in place concurrent with scheme launch. Those favoring "market driven" evolution to interoperability assume, incorrectly IMO, that such will occur in a manner similar to that experienced in the ATM and POS systems of the 1980s and 1990s. Trouble is that, for the most part, those services were virtually generic in nature and interoperability was created to expand scheme footprints and customer convenience. Here, where the solutions are heterogeneous, an entirely new set of technical and business hurdles will have to be overcome by market-driven decision-makers. If true, evolutionary interoperability (and its governance) could take far longer than the twenty-year experience with ATMs and POS systems.

Describe governance in more detail.

I would have liked to see some 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.

The governance portion of this proposal needs to be formalized before any meaningful comments can be made. That being said, end-users need a voice in the governance structure to voice their unique perspective. This needs to occur at every level to ensure the needs of end-users are represented appropriately.

G.1 Effective governance, Somewhat Effective & and G.2 Inclusive governance - Somewhat Effective. “A FAST Network Central Authority must oversee certain aspects of the Solution, including the vetting of the members and the authoritative control mechanism over enforcing members’ rules of engagement. Central Authority must be representatives of various central banks and/or banking institutions to promote comfort with adoption, especially in foreign countries that may be skeptical of a solely U.S.-controlled platform.”

Limiting the governance structure to FAST members will both inhibit adoption as well as create barriers for some stakeholders. I suggest the structure be expanded to include all stakeholder into the voting and decision-making process.
The governance outlined in the proposal does not state that all stakeholder groups will have proportional influence over the governance of the solution. This is in contrast to many other proposals, which did contain that language.
Proposer responses to the Task Force comments were optional and not all proposers chose to respond.
Faster Payments QIAT

FINAL 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

FINAL ASSESSMENT

Proposer: World Currency USA, Inc.

Summary Description of Solution:

World Currency USA’s solution, called FAST for the interim, allows contractually bound member-participants (i.e., financial institutions) to connect to each other through a web-based, front-end platform and to clear and settle payments through the establishment of FAST in-process clearing accounts at each member. A separate, web-based, front-end platform allows end-users to initiate and view their transactions in real time.

The FAST solution proposes to consolidate the notion of domestic Automated Clearing House (ACH) and wire payments into a single payment solution for domestic and cross-border payments. During its initial stages, FAST would operate in parallel with the existing payment platforms to facilitate adoption and avoid disruption. During this stage, FAST would employ a “least-cost routing” approach to payments. Existing platforms would then be used if they are preferred or if they are the only feasible option (such as when a bank is not a member of FAST).

A FAST Network Central Authority oversees the solution, including vetting its members and enforcing member rules. World Currency recommends that the Central Authority comprise central banks and/or other banking institutions; in places (e.g., p. 53), the proposal presumes that the Federal Reserve will run the FAST Network Central Authority.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major Strengths

– FAST consolidates payments into a single solution that enables payment at different speeds (e.g., faster payments, ACH, wire) for both domestic and cross-border transactions

– The solution can route transactions when possible and/or desired through a “least-cost-routing” approach that uses the ACH to reach payees who are not part of the FAST network.

– The solution has cross-border functionality that uses an intelligent matching algorithm that enables currencies to be sourced by other peer network members before being sent to the currency exchange market for fulfillment.

■ Areas for Improvement and Enhancement

– The solution proposes to create a new global network, but its advantages over existing networks are not clear. Clearly articulating those advantages will be critical to motivating providers to participate and make the solution available to end-users

– Because it is bank-centric, FAST is less accessible to non-banks than current offerings. Regulated Non-bank Account Providers can participate through one of the solution’s banking relationships, but banks need to be motivated to enable non-banks to participate.

– The solution allows member-banks to control the end-user’s experience, but more clarity is needed as to how the solution will require and enforce any base-level operating rules that would ensure minimum standards in feature functionality and/or a user experience that is consistent in its usability and predictability.

– More clarity is required on the solution’s settlement approach for money moved between members (not just for information exchanged through clearing).

■ Use cases addressed
The solution addresses all use cases—B2B (business to business), B2P (business to person), P2B (person to business), and P2P (person to person)—for both domestic and cross-border payments.

**Proposer’s overall ability to deliver proposed solution**

- The solution is based on hub-and-spoke models used in payment systems today, so its concepts are proven.
- Patents for components of the solution have been filed, but the full technical solution, including software and platform, has not yet been developed.
- The solution’s implementation plan is articulated only at a high level and needs more detail to substantiate its feasibility.
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 is accessible to any financial institution (FI) but requires non-banks to gain access through a bank partner (U.1.1). The solution is able to reach all payees who have a banking account—either through their member banks or by interoperating with existing payment systems, such as same-day ACH (U.1.2). If a payee is a customer of a non-member financial institution, the payer’s member-bank may originate the payment into the Federal Reserve System via the ACH network. The solution supports multi-currency transactions (U.1.3).

While the proposal states that Regulated Non-Bank Account Providers can access the solution through banking relationships, the solution does not address the needs of the unbanked, as users must have a bank account (U.1.4). More detail is needed as to how banks would be motivated to provide access to non-banks (U.1.1).

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 is available 24x7x365 through multiple channels, including web, call center, fax, in-person, and mobile (U.2.1, U.2.3). However, it is up to members to make FAST available to their end-users; if a member does not provide services 24x7x365, then the FAST solution might not be available 24x7x365 either. An adoption time frame will likely be set up wherein members will have a grace period while working towards 24x7x365.

The solution does not enable the initiation of payments with limited payee information, as it requires the payer to know the payee’s checking account number and the receiving bank-member’s FAST identifying number to make a payment (U.2.2). It offers a way to mask accounts through a random, unique character sting code that expires, but the solution would be more usable if end-users could use an alias to send payments. More clarity is needed as to how end-users might send payments using an alias.

The solution does not provide any requirements or enforcing mechanisms related to accommodating varying levels of technological proficiency and usability needs among end-users (e.g., the disabled, the elderly, and those with limited English-language proficiency) (U.2.4).

U.3 Predictability

<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 design delivers the defined baseline of core features and supports the communication of these baseline features to end-users (U.3.1-2). It also uses standard, web-
based communication and messaging protocols (U.3.3). The solution is described by the term “FAST” (U.3.6).

The proposal could be strengthened by describing in greater detail how the solution will require and enforce a predictable user experience, such as through guidelines or operating rules for providers (U.3.2, U.3.4). Additionally, the proposal notes that the originating member is liable for funds transmitted in all cases, but more detail is needed on the protections, rights, and liabilities of the payer and payee in cases of payment errors (U.3.5).

U.4 Contextual data capability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale**

The proposal indicates that the solution will use ISO 20022, but it also notes that message format specifics are still being architected (U.4.1). Custom programming will be used for direct integrations with business and personal finance systems, although baseline platform capabilities will include a CSV (comma-separated values) download of raw transaction information (U.4.2). Standards will be balanced with flexibility through a message format that supports an extensible set of addendum data records with a prefixed namespace to ensure unique tagging (U.4.3).

The solution is still architecting and developing its full set of contextual data capabilities. The proposal would be enhanced by providing more details about the design of the contextual data, including how the proprietary format referenced for contextual data will serve as a wrapper for ISO 20022 (U.4.1, U.4.3).

U.5 Cross-border functionality

<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 cross-border payments using a matching algorithm that reduces conversion costs by sourcing currencies from other, peer network members before sending them to the currency exchange market for fulfillment. Nostro accounts held at in-network member institutions in the name of the FAST Central Authority for each foreign currency are used to expedite the payment process by allowing immediate funds availability even before the matching algorithm has been completed (U.5.1). Interoperability with other payment systems will rely on the traditional methods of executing cross-border payments with non-FAST banks (U.5.2). The solution requires advance disclosure of fees, exchange rates, and other end-user costs (U.5.3) and enables currency conversion (U.5.4).

The solution embeds some of its cross-border functionality into the overall implementation timeline, but more detail is needed as to how the solution will achieve adoption and ubiquity for cross-border payments (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 can apply to a broad range of use cases. Once contextual data capabilities have been designed, the solution’s applicability to business payments will become clearer.

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 enables competition by allowing members to add their choice of providers and by letting end-users choose any member or any Regulated Non-Bank Account Provider (through a member) as their provider (E.1.1). The solution allows providers of any size to become a member as long as they meet participation requirements (E.1.4). Providers can make disclosures to end-users through the solution’s web-based, front-end platform (E.1.3).

The proposal can be strengthened by describing how non-banks can access the solution through banks (E.1.1), how end-users would designate the provider account into which they want to receive money, and how end-users could easily switch providers or use multiple providers (E.1.2).

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:
The solution uses open, accessible standards to help its members integrate and offer value-added services (E.2.1). Providers may offer value-added features as long as they meet participation requirements (E.2.2). The solution needs to ensure that members clearly disclose to customers that the value-added services are optional; the proposal mentions that this requirement could be included in the contractual arrangements (E.2.3).

The proposal makes limited mention of APIs and instead focuses on the solution’s web-based platform, which would make services essentially identical among providers. This approach may make it difficult for providers to differentiate and compete, even if they set prices. More detail is needed on the potential opportunity for providers to use APIs to design their own interface and to differentiate on that basis. Additionally, more information would be helpful on the type of messaging/information flow that is planned for the system, which would help to enable differentiating services.

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 solution provides a four-phase, two-year implementation timeline that includes: Phase 1: establishment of the FAST Network Central Authority and development of the software and
platform (9-12 months); Phase 2: evaluation of the security and control environment and test pilot with early adopters (6 months); Phase 3: live pilot with early adopters (6 months); and Phase 4: aggressive growth plan (ongoing).

Based on historical case examples, this timeline is considered to be aggressive. More details on the implementation plan are needed, such as: (1) how the solution’s implementation will be funded (the proposal indicates that it could be funded by venture capital or a newly formed entity), (2) the particular entities that WCUSA expects to adopt FAST, (3) implementation and ubiquity hurdles that might arise and how WCUSA will overcome them (e.g., achieving adoption, engaging both domestic and foreign banks), and (4) market share and growth projections. While a portion of the technology already exists, the business plan for adoptability is still in progress.

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:

The proposal states that FAST’s proprietary message format is interoperable with other, standard formats and will enable cross-border interoperability with ISO 20022; however, the format is still under development (E.4.1-2).

As such, more detail is needed on how ISO 20022 will be implemented with the proprietary format (E.4.1). It would likewise be helpful to understand whether the format is as cost-effective as standard formats for members (E.4.3). As a proprietary format, the messaging format is not developed or published by a recognized standards development organization, according to the proposal (E.4.5).

E.5 Comprehensiveness

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

In concert with its members, the solution supports every step of the end-to-end payment process, from initiation to reconciliation (E.5.1). 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 solution indicates that its technical requirements would support thousands of concurrent messages per second (E.6.1). It would be helpful to understand, however, the solution’s stress-tested capacity (E.6.2) and how the solution’s technical design can scale at peak times, as well as how the solution can adapt to ongoing developments (E.6.3).
E.7 Exceptions and investigations process

**Very Effective**  **Effective**  **Somewhat Effective**  **Not Effective**

**Rationale:**
The solution enables members to view their own transactions and to initiate investigations with the FAST Network Central Authority (E.7.1). A web-based platform allows members to flag transactions for review, send alerts, and correspond in order to address exceptions or disputes. The FAST Central Authority has the final say in settling disputes. Members have access to a centralized transaction log to support error resolution; all records are stored for at least 10 years (E.7.2). The solution does not yet aggregate exceptions data to spot patterns across participants, but the proposal indicates the intention to offer this capability during the implementation phase (E.7.3).

Further detail would be helpful on the solution’s protocols and timeframes for addressing exceptions (E.7.1).

Safety and Security

S.1 Risk management

**Very Effective**  **Effective**  **Somewhat Effective**  **Not Effective**

**Rationale:**
The FAST Central Authority will implement a formal Risk Management and Information Security Program. The solution will undergo regular third-party assessments of its operational and technical control environment (S.1.3, S.1.6).

The proposal does not define a risk management framework with rules, policies, and procedures to address the risk posed by an unexpected application of a law or regulation; risks related to settlement; operational risks; and risks posed by unauthorized, fraudulent or erroneous payments. The proposal does not describe any incentives offered to operators and providers to address and contain the risks they pose to other participants (S.1.1-S.1.6).

S.2 Payer authorization

**Very Effective**  **Effective**  **Somewhat Effective**  **Not Effective**

**Rationale:**
The solution requires payers to authorize each payment to their member-bank at the time of payment initiation (S.2.1). FAST does not have pre-authorization capability (S.2.2-3).

S.3 Payment finality

**Very Effective**  **Effective**  **Somewhat Effective**  **Not Effective**
Rationale:
The payer’s member-bank approves each payment and assures the availability of good funds (S.3.1). The payment becomes irrevocable once it is authorized by the payer and released to the FAST Network (S.3.2). The solution gives members the ability to disclose all relevant consumer protection information to the payer when payments are disputed and holds the originating member responsible for compensating the payer.

More detail would be helpful on the dispute process; the proposal does note, however, that the FAST Central Authority will be the ultimate arbiter of disputes (S.3.3).

S.4 Settlement approach

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
This solution has outlined an approach to settlement that involves “in-process” or segregated accounts held at each member institution. The proposal notes that clearing of members takes place through the in-process account that is debited and credited, and that settlement occurs once the receiving member acknowledges acceptance of the incoming payment.

More clarity is needed on how money actually moves—the segregated account held at each member institution can be used to clear funds (by debiting and crediting a ledger), but net-receiving institutions will have an overhang of funds owed. The solution does not detail how money will move from one provider to another, or how the settlement risk is managed.

S.5 Handling disputed payments

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
The solution provides the platform and tools required for members to comply with consumer error resolution and consumer protection laws (S.5.2). The platform also enables a payer to request a voluntary return of funds from the payee (S.5.3).

While the proposal indicates that the solution will have a participation agreement that defines the requirements, processes, and timeframes for disputed payments or mechanisms, the agreement is still under development (S.5.1, S.5.4-5).

S.6 Fraud information-sharing

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
The solution shares real-time information on successfully executed transactions through its web-based platform (S.6.1). It supports differential access to content based on the roles and responsibilities of its operators, providers, and regulators (S.6.5). The FAST central authority stores and aggregates this information (S.6.6).

The solution does not yet collect the type of information needed—such as data on rejected transactions—to manage and monitor fraud (S.6.1), and the proposal does not specifically
describe plans to do so in the future. The solution does not require member-banks and participants to share fraud-related information (S.6.1), nor does it leverage fraud-related data from other entities to share with operators and providers (S.6.2). FAST does not support real-time and ex-post management and monitoring of fraud, nor does it provide timely updates and alerts (S.6.3). Rather, the solution “supports real-time access of payment data to all relevant parties” (p. 53). Finally, the solution does not yet aggregate and analyze fraud information to spot patterns across participants (S.6.7); participants are expected to rely on “data extracts and third-party integrations” to perform this function themselves (p. 54).

S.7 Security controls

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution will have an Information Security Program to assess and manage risks and to set policy for information handling and personnel, as well as an Operations program to detail policies and procedures.

The proposal thus acknowledges a need for security controls and sets out a development path for them during the implementation phase, but development is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

S.8 Resiliency

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposal provides an overview of the solution’s approach to resiliency. A declaration team will be established at the FAST Central Authority, and as well as a Disaster Recovery Lead will be appointed to oversee the solution’s business contingency program (S.8.4).

Given this, the proposal acknowledges a need for resiliency and sets out a path to ensure it during the implementation phase, but robust resiliency is not yet in place. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

S.9 End-user data protection

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The authentication and user-based permission sets in the front-end FAST platform provide operators and providers with robust controls and mechanisms to protect sensitive information (S.9.1).

The solution indicates that sensitive information like account numbers can be protected through single-use codes that enable account-masking (S.9.2-3). While this capability can support end-
user data protection, it complicates what is meant to be a straightforward, simple end-user experience.

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:**

The solution has a robust framework and mechanisms for identification and verification as it enrolls end-users and providers and facilitates transactions (S.10.1). The payee’s provider must communicate acceptance of a payment before finalizing the transaction (S.10.2). These mechanisms and framework align with regulatory guidance and industry standards (S.10.3). End-users are authenticated initially to the solution, and FAST requires providers to re-authenticate end-users when needed (e.g., if the session expires due to inactivity) (S.10.5). Authentication models can also be changed if the threat landscape changes (S.10.6).

The solution itself does not control authentication; members authenticate end-users and select their own authentication controls. More information is therefore needed on how the solution would enforce these controls. In addition, it is not clear whether authentication and re-authentication can be varied based on risk-weighting or any other factors for all consumer and business transaction types (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 FAST Network Central Authority vets new member-banks before they can become members and maintains member records and status (S.11.1-2). The Authority will also be responsible for upkeep of member records and status (S.11.3).

The proposal does not address processes to regularly monitor and ensure members’ compliance with the participant 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 enables approval within two seconds for in-network payments, but it allows members to set parameters for additional, self-imposed internal controls based on risk. These additional controls (e.g., dual authorization) could increase the approval process time. Thus, the operator, provider, and operating rules ultimately control the speed of approval.
F.2 Fast clearing

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale:**
The solution enables clearing within two seconds for in-network payments, but, as mentioned above, it allows members to set parameters for additional, self-imposed internal controls based on risk. These added controls (e.g., dual authorization) could increase the approval process time and thus impede clearing speed. Thus, the operator, provider, and operating rules ultimately control the speed of clearing.

F.3 Fast availability of good funds to payee

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale:**
The solution enables availability of funds within one minute for in-network payments, but as mentioned above, it allows members to set parameters for additional, self-imposed internal controls based on risk. These additional controls (e.g., dual authorization) could increase the approval process time and hence the speed of funds availability. Thus, the operator, provider, and operating rules ultimately control the speed of funds availability.

More clarity is needed as to whether the funds from cross-border payments would be available within four hours or within the shorter time frame that the proposal indicates is possible.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale**
As with S.4, the solution has outlined an approach to settlement that involves “in-process” or segregated accounts held directly at each member institution. The proposal notes that clearing of members is done through the in-process account that is debited and credited, and that settlement occurs once the receiving member acknowledges acceptance of the incoming payment.

It would be helpful to understand how money actually moves. The segregated account held at each member institution can be used to clear funds (to debit and credit a ledger), but the proposal needs to detail how the money moves from one provider to another—whether through Central Bank money or commercial bank money—and how the settlement risk is managed (F.4.1, F.4.3).

F.5 Prompt visibility of payment status

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**
Rationale:
The solution provides member-banks with “real-time status updates at each stage of the transaction” (p. 57), but it is up to each member to determine whether and when the payer and payee have visibility into payment status.

**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:**
The solution identifies relevant legal sources (L.1.1) and identifies a gap in covering consumer protections for cross-border payments, with a plan to address this gap (L.1.2). Members are contractually and legally obligated to adhere to the solution’s rules (L.1.3).

The proposal does not describe the main components and dimensions of the legal framework. The solution supports legal and regulatory compliance related to OFAC screening (L.1.4) and does not foresee any unique legal provisions that would be needed to address situations in which parties perform the same function but are subject to different laws or regulations (L.1.5). However, as cross-border payments are a target use case, the solution should consider how it will support compliance with relevant U.S. law by all end-users and providers, particularly in cases of conflicting laws. Similarly, the solution does not address how it will reconcile U.S. rules with non-U.S. regulated providers in cross-border payments.

**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 proposal acknowledges a need for payment system rules and sets out a path to complete them during the implementation phase, but these rules are is 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 proposal acknowledges a need for an approach to consumer protection and sets out a path to develop it during the solution’s implementation phase, but the approach is 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.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 proposal acknowledges the need for an approach to data privacy and sets out a path to complete it during the implementation phase, but the approach is 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.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 solution’s approach to intellectual property rights addresses all risks arising from third-party rights related to patents, trademarks, copyrights, and trade secrets. The approach resolves or manages these risks prior to implementation.

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’s governance approach includes public disclosure of governance arrangements (G.1.2) and provisions for independent validation of compliance with the solution’s rules, applicable law, and achievement of objectives (G.1.4).

While the proposal describes a central governance authority, it does not address “efficient decision-making and rule-making” or define policies and structure (G.1.1). Because the solution plans to define the appeals process during implementation, the proposal does not include information on the process (G.1.3).

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 proposal acknowledges a need for inclusive governance and sets out a path to complete an inclusive governance model during the implementation phase, but the model is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”