Faster Payments QIAT

Proposer: WingCash

February 21, 2017

TABLE OF CONTENTS

Original Proposal 2

Q&A Response 169

Draft QIAT Assessment 191

(Includes proposer comment in Appendix A & B) 207

Task Force comments 210

Proposer response to Task Force comments 220

Final QIAT Assessment 233
Faster Payments Network

Solution Proposal – Faster Payment Task Force

April 29, 2016
Submitted by: W. Bradley Wilkes, WingCash
# Contents

Acknowledgments.............................................................................................................................................. 6  
Solution Proposal Authors and Contributors .............................................................................................. 6  
Open Source Implementation Authors and Contributors .............................................................................. 6  
Executive Summary .................................................................................................................................... 7  
Introduction.................................................................................................................................................. 7  
The Faster Payments Network End-to-End Description ............................................................................... 8  
Main Improvements of the FPN ................................................................................................................ 8  
Gaps and Opportunities in Current Payment Systems ................................................................................ 9  
Finality, Validation of Available Funds, Real-time Posting and Availability of Funds ......................... 9  
Timely Notifications .................................................................................................................................. 9  
Masked Account Details ............................................................................................................................ 10  
Integration with Mobile Devices and Digital Wallet Providers ................................................................. 10  
Integration with Accounting Systems and Money Management Programs ......................................... 10  
Transparency in Fees and Timing of Cross-Border Payments ................................................................ 10  
Baseline Features Defined and Description of Payment Flow ................................................................ 11  
Conclusion .................................................................................................................................................. 11  
Use Case Coverage .................................................................................................................................... 12  
Supported Use Case Coverage Summary ................................................................................................ 12  
Cross-Border Use Case Coverage ........................................................................................................ 13  
Proposal Assumptions ............................................................................................................................... 14  
Part A: Detailed End-to-End Payments Flow Description ....................................................................... 15  
Part A, Section 1: Solution Description ...................................................................................................... 15  
  Detailed End-to-End Solution Description ............................................................................................... 15  
  FPN End to End Functional Overview .................................................................................................... 16  
  Definition of Stakeholder Roles and Responsibilities ............................................................................ 17  
  Enrollment ............................................................................................................................................... 18  
  Persons and Businesses Have Limited Ability to Hold and Transfer Funds ....................................... 22
Ongoing Efforts to Resist Threats and Attacks .......................................................... 22
Authentication .................................................................................................................. 23
Payment Orders (includes Initiation & Payer Authorization) ............................................ 25
Receipt (Clearing, Settlement, and Notification) .............................................................. 35
Optional Payment Codes ................................................................................................. 38
Return of Payment Received in Error .............................................................................. 42
Reconciliation .................................................................................................................. 42
Approval by the Payer’s Provider .................................................................................... 44

Part A, Section 2: Use Case Description ........................................................................ 44

Person-to-Person .............................................................................................................. 45
Person-to-Business ......................................................................................................... 45
Business-to-Person .......................................................................................................... 46
Business-to-Business ....................................................................................................... 47

Part A, Section 3: Use Case by Effectiveness Criteria .................................................... 47

Part B: Business Considerations .................................................................................... 49

Interoperability .............................................................................................................. 49
Interoperable with the ACH Network .............................................................................. 49
Interoperable with Payment Card Networks .................................................................. 49
Interoperable with Other Payment Networks ............................................................... 50

Implementation Timeline .............................................................................................. 50
Technical Features in the Current Open Source Implementation .................................... 52
Technical Features at Implementation of FPN ............................................................... 53

Value Proposition and Competition ............................................................................. 53
Value Proposition for the Federal Reserve ...................................................................... 53
Value Proposition for Depository Institutions .............................................................. 54
Value Proposition for Regulated Non-Bank Providers .................................................. 55
Value Proposition for Businesses ..................................................................................... 56
Value Proposition for Persons ......................................................................................... 57
Value Proposition for Integrators ................................................................................................................. 58
Integration Effort .................................................................................................................................................. 59
Points of Integration ........................................................................................................................................... 59
Relative Effort Required for Integration by Stakeholder .................................................................................. 61
Business Relationships Between Stakeholders ................................................................................................. 61
Part C: Self-Assessment Against Effectiveness Criteria .................................................................................... 62
  Part C, Section 1: Ubiquity ................................................................................................................................. 62
    U.1, Accessibility ............................................................................................................................................... 62
    U.2, Usability ..................................................................................................................................................... 73
    U.3, Predictability ............................................................................................................................................. 76
    U.4, Contextual Data Capability ..................................................................................................................... 79
    U.5, Cross-Border Functionality ..................................................................................................................... 80
    U.6, Applicability to Multiple Use Cases ....................................................................................................... 82
  Part C, Section 2: Efficiency .............................................................................................................................. 84
    E.1, Enables Competition .................................................................................................................................. 84
    E.2, Capability to Enable Value-Added Services ............................................................................................ 88
    E.3, Implementation Timeline ......................................................................................................................... 90
    E.4, Payment Format Standards .................................................................................................................... 95
    E.5, Comprehensiveness .................................................................................................................................... 96
    E.6, Scalability ................................................................................................................................................ 97
    E.7, Exceptions and Investigations Process .................................................................................................. 99
  Part C, Section 3: Safety and Security ................................................................................................................ 100
    S.1, Risk Management .................................................................................................................................... 100
    S.2, Payer Authorization ................................................................................................................................ 104
    S.3, Payment Finality ....................................................................................................................................... 106
    S.4, Settlement Approach ............................................................................................................................... 107
    S.5, Handling Disputed Payments .................................................................................................................. 108
    S.6, Fraud Information Sharing ...................................................................................................................... 110
S.7, Security Controls ............................................................................................................................................. 113
S.8, Resiliency .......................................................................................................................................................... 122
S.9, End User Data Protection .................................................................................................................................. 124
S.10, End User/Provider Authentication .................................................................................................................. 126
S.11, Participation Requirements .................................................................................................................................. 130
Part C, Section 4: Speed (Fast) ....................................................................................................................................... 132
  F.1, Fast Approval .................................................................................................................................................. 132
  F.2, Fast Clearing ................................................................................................................................................... 132
  F.3, Fast Availability of Good Funds .......................................................................................................................... 132
  F.4, Fast Settlement .................................................................................................................................................. 133
  F.5, Prompt Visibility of Payment Status .................................................................................................................. 134
Part C, Section 5: Legal Framework .............................................................................................................................. 135
  L.1, Legal Framework ............................................................................................................................................. 135
  L.2, Payment System Rules ....................................................................................................................................... 151
  L.3, Consumer Protections ....................................................................................................................................... 156
  L.4, Data Privacy ....................................................................................................................................................... 157
  L.5, Intellectual Property ......................................................................................................................................... 159
Part C, Section 6: Governance ....................................................................................................................................... 160
  G.1, Effective Governance ......................................................................................................................................... 160
  G.2, Inclusive Governance ......................................................................................................................................... 162
Glossary of Terms ............................................................................................................................................................ 165
ACKNOWLEDGMENTS

Solution Proposal Authors and Contributors
W. Caleb Brigman
Andrew D. Callister
Kendall Chadwick
Jacob Christensen
Janet O. Estep
Benjamin Geva
Alexis L. Hales
Shane Hathaway
Michael C. Johnson
Spencer D. Marks
Paul Proctor
Jennifer Taylor
David E. Teitelbaum
Stephen Wallant
Braxton C. Wardle
W. Bradley Wilkes
Colbrin A. (Colby) Wright

Open Source Implementation Authors and Contributors
Randall Bohn
Steve Curtis
Shane Hathaway
Todd Millecam
Daniel Roper
B. Bradley Wilkes
W. Bradley Wilkes
Cody Wilson

Thanks also to all those individuals not named here who contributed to the following applications included in our open source application stack: PostgreSQL, RabbitMQ, Python, Pyramid, SQLAlchemy, Memcached, Buildout, Twisted, Ionic, and many more open source projects. We are enormously grateful for all the foundational work.
EXECUTIVE SUMMARY

Introduction

We are pleased to present a solution proposal for a new Faster Payments Network (FPN) to improve the U.S. payments system and to reestablish the United States as a leader in the “instant economy”\(^1\) globally.

The Faster Payments Network proposed herein (a) reduces the societal costs of payments, (b) combines optimal payment speed (i.e., immediate) with improved payment security, (c) makes access freely available to U.S. consumers, including the underserved and unbanked, and businesses, including financial institutions and government organizations, (d) builds on the strength and understanding of the United States dollar, (e) expands the reach and influence of the United States dollar, (f) addresses the gaps in current payment systems, and (g) provides incentives for depository institutions, businesses and consumers to voluntarily participate.

The author believes that to achieve the public policy goals stated in the Federal Reserve’s Strategies for Improving the U.S. Payment System paper\(^2\) while, at the same time, balancing various stakeholder interests and satisfying various stakeholder expectations requires a combined public and private ownership structure and the implementation of a proven governance model for the Faster Payments Network.

In addition to recommending a public/private ownership structure, the solution proposal identifies roles and responsibilities for the Federal Reserve and the Department of the Treasury. The solution proposal also specifies the extension of the FedCash Service to include the authoritative issuance of digital bills and coins (Fed notes) with a complementary and tightly integrated Global Directory Service (GDS). The author’s inclusion of the roles and responsibilities for the Federal Reserve and Department of the Treasury and extension of the FedCash service and addition of a Fed Global Directory Service belong solely to the author. Neither the Board of Governors of the Federal Reserve system or any employee of the Federal Reserve System or any employee of any of the Federal Reserve Banks nor the Department of the Treasury or any employee of the Department of the Treasury have in any way committed to provide the services described herein.

This solution proposal and the current open source implementation\(^3\) from which the technical designs are included are the cumulative result of thousands of hours of work by many. The primary author of the solution proposal has made every effort, in gratitude, to include the names of all those who have contributed to both the solution proposal and the open source implementation in the acknowledgements section.


\(^3\) The current version of the open source implementation can be freely downloaded at wingcash.org.
The Faster Payments Network End-to-End Description

The solution is a software platform, referred to as the Faster Payments Network (FPN), under the combined ownership and operation of the Federal Reserve (the Fed) and the Governing Organization (GO). A key innovation of the FPN is its method to deliver final payment. The method to deliver final payment is to allow the Federal Reserve to authoritatively issue Federal Reserve notes (Fed notes) that are affixed to a single Internet domain (e.g., fednotes.net) and remain under the Federal Reserve’s control while simultaneously allowing persons and businesses to hold, transfer possession of and/or deposit the Fed notes.

Another vital innovation of the FPN is its use of Uniform Resource Locators (URL’s) for the GDS. The use of a URL provides a secure context for each entry in the GDS, allows the GDS to interact with end users and to interoperate with many other types of things (e.g., vending machines, printers, ATMs, change dispensers and more).

The end-to-end payment process begins with a person or business completing a one-time enrollment in the FPN and continues through the iterative steps of authentication, payment order, receipt and an optional reconciliation step (see Part A, Section 1: Solution Description on page 15).

The current open source implementation of the FPN has been in operation in local markets since 2011 with fully developed and market-tested features (see Part B, Business Considerations). Although the current implementation of the FPN is an open source application stack, the author recommends the conversion of the stack from open source applications to equivalent proprietary applications that provide strong operational and quality control over the application stack’s source code.

Main Improvements of the FPN

The following list highlights the main improvements the FPN achieves over existing payment systems:

- **Access** to the FPN is freely available to all US consumers and businesses without the requirement for credit scores, credit histories or accounts with depository institutions.
- The FPN centrally records changes in possession of Fed notes immediately and in real time.
- Similar to the transfer of possession of physical notes, the FPN can be used for *in-person* transfers (i.e., P2P, P2B, or B2P) using a supported device and an Internet connection.
- Similar to other electronic payments systems, the FPN can be used for *remote payments* for all targeted use cases.
- Similar to the change of possession with physical notes, changes in possession on the FPN occur directly between payer and payee *without transfer fees*.

---

4 The FPN’s technical design supports fees for certain transfers (e.g., from a business to an account at a depository institution).
• The FPN supports the roles and responsibilities of the stakeholders in the physical currency system (i.e., Federal Reserve, depository institutions, Department of the Treasury).
• The holders of Fed notes on the FPN can both visually and cryptographically validate the authenticity of the Fed notes.
• The holders of Fed notes on the FPN may deposit the notes into their own account with a depository institution.
• The FPN’s design principle that allows the Federal Reserve to issue Fed notes also allows businesses to issue closed-loop notes, also called brand cash, denominated in USD to support gift, loyalty, reward, promotional, humanitarian and welfare programs.
• The FPN allows for rich contextual data (e.g., invoice, geolocation, order information) to be associated with the payment.
• The FPN supports the transfer of value in denominations as small as $.01 USD.
• The FPN’s business model makes it cost-effective to transfer value in denominations as small as $.01 USD.
• The FPN is available 24x7x365.
• The FPN does not require the Payee to receive and to protect sensitive account information (e.g., payment card account number, checking account number) from the Payer.

Gaps and Opportunities in Current Payment Systems

The FPN’s features address the following gaps in current payment systems: (a) finality, (b) validation of available funds, (c) real-time posting and availability of funds, (d) timely notifications, (e) masked account details, (f) integration with mobile devices and digital wallet providers, (g) integration with accounting systems, and (h) the lack of transparency in fees and timing for cross-border transfers.

Finality, Validation of Available Funds, Real-time Posting and Availability of Funds

The transfer of digital Fed notes in the FPN is reliable and immediate just like the transfer of physical Fed notes (i.e., cash). The FPN ensures that only good funds are used for payments. Because a Payer using the FPN is only authorized to transfer Fed notes he holds, Payees can be certain they are receiving good funds for payment and are receiving them from a Payer authorized to make the payment. Additionally, the transfer of Fed notes in the FPN is immediate and makes funds available to the Payee upon receipt.

Timely Notifications

The FPN allows timely notification of payments because it is connected to various external communication channels, including email, SMS/text message, social media sites, and within an

---

5 Payment System Improvement - Public Consultation Paper, The Federal Reserve Banks, September 10, 2013, p. 3
app on a smart device. The FPN notifies both the Payer and the Payee at the completion of each transfer, when funds are available to the Payee.

**Masked Account Details**

The FPN’s technical design specifies a system of various types of Uniform Resource Locators (URLs). The use of URLs allows the FPN to map a URL to a resource like a bill, a coin, an account at a depository institution, a vending machine, or other everyday physical objects. When the end user of the FPN has permission to use a resource, like an account at a depository institution, the FPN provides access to the resource through its URL. In this way, account details are masked when used in the FPN. The proposal also refers to a URL mapped to a resource as a payment address or payment address alias. The collection of payment addresses and payment address aliases is the Global Directory Service (GDS).

**Integration with Mobile Devices and Digital Wallet Providers**

The FPN’s technical design utilizes Internet data streaming standards and an Application Programming Interface (API) to both decrease cost and simplify integration for mobile devices and digital wallet providers. The FPN also defines a variety of function calls in the API to support integration of the baseline features and value-added features into mobile devices and digital wallets.

**Integration with Accounting Systems and Money Management Programs**

The FPN’s technical design supports the association of rich contextual data with payment information. Contextual data that can be included with the payment include complete invoice information, complete order information, and more. The API also makes it possible for payment information and contextual data to be exported for use in both large and small accounting systems and money management programs. The FPN’s use of Fed notes with rich contextual data in connection with the API enables low-cost integration with accounting systems and provides a compelling value proposition for businesses to switch from check-writing to more efficient transfers using the FPN.

**Transparency in Fees and Timing of Cross-Border Payments**

The FPN’s technical design also addresses transparency in fees and timing of cross-border payments. The FPN’s use of fednotes.com and Fed notes for payments makes it simple for immediate, real-time transfers to cross geographical borders. Furthermore, the FPN supports all currencies. Transfers are completed in a single currency, but Payers and Payees can convert currency they hold at any time. The FPN discloses conversion fees to be paid by the party converting currency.
Baseline Features Defined and Description of Payment Flow

The FPN allows persons and businesses to hold and transfer digital Fed notes for payment, with the direction of payment flow from the Payer directly to the Payee.

For example, the FPN specifies a single Internet domain (e.g., fednotes.com) where the Federal Reserve publishes digital bills and coins (Fed notes). Each Fed note is a unique web page with an immutably assigned URL that includes both a currency code (e.g., USD) and a unique identifier similar to a serial number (e.g., ML14060622C). Combined, these components form a unique, immutable address for each Fed note published at fednotes.com (e.g., fednotes.com/usd/ml14060622c).

In addition to the URL, each Fed note is assigned a single, permanent, monetary unit of value (e.g., $.01 to $100). Each Fed note also has a field that stores the URL of the issuer (e.g., fednotes.com/federalreserve) and a field that stores the URL of the current holder (e.g., fednotes.com/user/ericjones or fednotes.com/business/walmart).

The URL that points to the current holder of the Fed note is an endpoint that has the end user’s identity and credential associated with it. The FPN’s technical design allows only the Fed note’s current holder, who has authenticated to the network, to transfer possession of the Fed note to another entity.

For example, suppose the Federal Reserve issued a $1.00 Fed note using the FPN. Jane Smith has enrolled in the FPN. Joe Smith, Jane’s spouse, has also enrolled in the FPN. Jane authenticates to the FPN, and the FPN shows her that she holds $1.00. She instructs the FPN to transfer the $1.00 Fed note she holds to her spouse, Joe. The FPN updates the possession attribute of the Fed note from Jane to Joe, and the transfer is complete. The payment flow is directly from the Payer, Jane, to the Payee, Joe. As another option, Jane could transfer a Fed note she holds to her local grocer or her financial institution.

When a Fed note is transferred from one end user to another, it does not circulate or move in any way. Instead, the possession attribute that specifies who holds the Fed note is updated, and the Fed note is immediately available for use by the new Holder (the Payee).

Conclusion

The proposed Faster Payments Network is consistent with the role the Federal Reserve envisions for itself in the U.S. payment system. The Policy Statement\(^6\) for the Federal Reserve regarding its role in the payments system states that the role of the Federal Reserve in providing payment services is:

To promote the integrity and efficiency of the payment mechanism
To ensure the provision of payment services to all depository institutions on an equitable basis and to do so in an atmosphere of competitive fairness.

The policy also states that as the Federal Reserve considers the introduction of new services or major enhancements, all of the following criteria must be met:

- The Federal Reserve must expect to achieve full recovery of costs over the long run.
- The Federal Reserve must expect that its providing the service will yield a clear public benefit, including, for example, promoting the integrity of the payment system, improving the effectiveness of financial markets, reducing the risk associated with payment and securities-transfer services or improving the efficiency of the payment system.
- The service should be one that other providers alone cannot be expected to provide with reasonable effectiveness, scope and equity. For example, it may be necessary for the Federal Reserve to provide a payment service to ensure that an adequate level of service is provided nationwide or to avoid undue delay in the development and implementation of the service.

We believe that the FPN meets each of these tests. By providing a fiat digital currency, the Federal Reserve will be providing a service that it is uniquely positioned to enable, that will facilitate clear public benefits through broad-based, non-discriminatory access to an efficient and effective means of electronic commerce and that will enable the Federal Reserve to continue to perform its core responsibilities in managing the money supply. The FPN is competitively neutral and cost-effective and will enable the Federal Reserve to continue to ensure the integrity of the payment system with modest changes to existing law. In short, we respectfully submit that the Faster Payments Task Force and the Federal Reserve should adopt the FPN as its primary initiative for payment system improvement.

**USE CASE COVERAGE**

**Supported Use Case Coverage Summary**

The following table summarizes the use cases covered by the FPN at implementation. The table also gives examples of payments supported for each supported use case.

<table>
<thead>
<tr>
<th>FPN Supported Use Cases at Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Case</strong></td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>Business-to-Business (B2B)</td>
</tr>
</tbody>
</table>
## Faster Payments Network Solution Proposal

### FPN Supported Use Cases at Implementation

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Supported</th>
<th>Cross-border</th>
<th>Examples of Payments Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business-to-Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>The FPN assists businesses and governments to make payments of all types to persons. Payments supported include: Social Security, government pensions, employee wages, welfare payments, tax refunds, salaries, expense reimbursements, and petty cash.</td>
<td>The FPN is suitable for all types of business-to-person payments. The FPN supports both remote and in-person payments as well as ad hoc low-value and high-value payments.</td>
</tr>
<tr>
<td>Person-to-Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>The FPN enables immediate, final payments from person-to-business for many types of payments, including payments for purchases, services, utilities, medical treatment, rent, repayment of loans, etc.</td>
<td>The FPN enables either remote or in-person payments in both low- and high-value amounts.</td>
</tr>
<tr>
<td>Person-to-Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>The FPN is ideal for person-to-person payments including remittances, gifts, debt payment, shared expenses, allowances, etc.</td>
<td>The FPN allows both in-person and remote person-to-person payments.</td>
</tr>
</tbody>
</table>

### Cross-Border Use Case Coverage

The FPN’s technical design allows for rules, regulations and laws to be incorporated into the logic of the network. The FPN’s technical design allows both sending and receiving transfers irrespective of jurisdiction and restricting transfers based on jurisdiction. In addition to jurisdictional restrictions, technical constraints may limit cross-border use case coverage, like Internet connectivity and possession of or access to supported devices.

In jurisdictions where transfers are permitted by local law, permitted under FPN rules and supported by local technological infrastructure (e.g., Internet connectivity and devices), the FPN supports that cross-border corridor.

Unless restricted by the FPN rules, all use cases will be covered at implementation. Integration with other payment systems (e.g., UK Faster Payments, Singapore FAST, SPEI, etc.) can be achieved by the operators of the other payment systems using the API. Other parties, including operators of other payment systems that integrate using the API, are required to have applications certified before the application can be published and released to end users. Applications that do not function according to FPN rules cannot be certified.
The proposed solution does not seek to eliminate physical cash any more than it seeks to eliminate other payment networks (e.g., ACH network or payment card networks). The features and functions of existing payment networks, like physical currency, are essential to the economic backbone of the economy. The solution does seek to make it possible for any entity to transfer value electronically using methods that seek to preserve and to emulate physical currency. The author believes that the adoption of the FPN presented herein will compete successfully with both the ACH network and the payment card networks and may cause the loss of revenue to financial institutions, the ACH network and payment card networks as payments shift to the FPN.

To achieve the widespread adoption that is equivalent to the universal acceptance of the U.S. dollar, the author believes that the notes (i.e., digital bills and coins) proposed should be issued by the Federal Reserve, become legal tender of the United States, and be called Federal Reserve notes (Fed notes). Therefore, the proposal refers throughout to digital bills and coins of the system as Fed notes. The FPN’s technical design also requires that each Fed note be given a URL at an Internet domain controlled and in-part operated by the Federal Reserve; therefore, the solution uses fednotes.net as an example Internet domain where Fed notes are issued. The author acknowledges that it is not a member of the Federal Reserve System (FRS) and that the solution relies on the expansion of FRS services. The Federal Reserve has not committed in any way to provide the services proposed herein.

The author believes that the Federal Reserve’s issuance of Fed notes is crucial to obtaining voluntary participation from depository institutions in the FPN. Depository institutions have an additional incentive to participate because they may earn fees when Fed notes are deposited.
The author also believes that the Department of the Treasury should maintain its role as the designer of Fed notes; therefore, the FPN’s technical design has a role and permissions for the designer of the Fed notes. The face of each Fed note also has a reference to the Department of the Treasury as the designer. The Department of the Treasury has not committed in any way to provide the services proposed herein.

The proposal also recommends the formation of a Governing Organization (GO) to function as the rule-making body and operate certain components of the FPN. The author recommends that members of the Faster Payments and Secure Payments Task Forces are grandfathered in as founding members of the GO with no membership fee until the service reaches ubiquity in 2020. The GO will have additional responsibilities as proposed in the Governance section (see Part C, Section 6). The author believes that the ownership, operating and governance model should be patterned after the ownership, operating and governance model for the ACH network.

The author believes that the FPN’s technical design is unique because it is architected to support multiple issuers of both national currencies and closed-loop value. The author’s references to the multi-issuer capabilities of the FPN in the proposal are limited to describing functional capabilities. Unless specifically indicated, the author does not imply specific relationships with any other parties, organizations, or governments used herein.

To assist assessors, the solution proposal includes a variety of short screencasts that are roughly one to two minutes long. These screencasts augment the written “what” and “how” descriptions of the proposed solution. When a published screencast is available, a link is located near the related description. The screencasts are created in a sandbox on the wingcash.org website and are intended to present realistic examples of how the FPN features operate in the current implementation; therefore, the screencasts may show or use the names of real organizations or persons in the examples. The use of the name of any real organization or person in a screencast is not a recommendation or endorsement by that organization or person for the proposal or the content herein but rather an authentic depiction of the features in the FPN.

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 life cycle.
- Section 2 focuses on the details of the solution by describing the solution’s supported use cases across the eight stages of the payment life cycle.
- Section 3 provides a summary table of whether the effectiveness criteria are addressed by each supported use case.

Part A, Section 1: Solution Description

Detailed End-to-End Solution Description

The solution proposal presents a detailed blueprint for establishing a Faster Payments Network (FPN) patterned after the form and function of physical bills and coins. The proposal presents carefully designed methods that seek to preserve many of the attributes and features of physical
currency as it is digitized. The authors prefer to focus the proposal on the FPN’s design, including the principles associated with the design and the technology that supports the design, rather than on its current implementation; however, nearly all examples are represented by the current implementation and are drawn from the current design and operating functions.

The FPN’s design supports client-server message flow for all communications and uses a distributed server farm and stateless process architecture to support scale. The FPN’s design facilitates all payments flowing directly from the Payer to the Payee. The following graphic illustrates the FPN’s network architecture.

The FPN’s design is based on a centralized service like those developed by Google, Amazon, Facebook and many other companies that have built successful centralized services. Centralized services have the advantage of being developed using Internet standards and draw from a broad base of developers who know how to design and code centralized services, ultimately reducing the cost of implementation, maintenance and update. Centralized services have repeatedly proven effective.

**FPN End to End Functional Overview**

The FPN’s technical design specifies a one-time enrollment step, three iterative steps (authentication, payment order, and receipt), and the final, optional step of reconciliation. The
functions of each step are described in greater detail below and represent the FPN’s end-to-end payment life cycle (see graphic below).

While the diagram above outlines the full payment sequence within the FPN, an end user does not need to complete an entire sequence with each session. For example, in one session an end user may authenticate just to submit a payment order, and in another session the end user may authenticate to visually confirm receipt of a payment. The receipt step does not require the Payee to be authenticated to the FPN.

**Definition of Stakeholder Roles and Responsibilities**

The FPN defines roles and responsibilities for stakeholders that participate in the FPN. The table below shows the FPN’s defined roles and responsibilities for each stakeholder:

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Roles &amp; Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Federal Reserve</td>
<td>The Federal Reserve is responsible for regulation, oversight, issuing and redeeming US dollars (Fed notes), operations, and financial responsibility in the case of failure of the Governing Organization.</td>
</tr>
<tr>
<td>Governing Organization</td>
<td>The Governing Organization has the roles and responsibilities of operator, compliance, rule making, financial responsibility for systematic errors, training, education, end user engagement, customer service, FPN administration, and hiring independent reviewers and auditors to assure compliance with rules.</td>
</tr>
</tbody>
</table>
## FPN Stakeholder Defined Roles & Responsibilities

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Roles &amp; Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depository Institutions</td>
<td>Depository institutions order and initially distribute Fed notes, accept Fed notes for deposit from their customers, and provide customer service. Depository Institutions are also end users.</td>
</tr>
<tr>
<td>Regulated Non-Bank Providers</td>
<td>Regulated non-bank providers accept Fed notes for deposit and provide Fed notes for purchase to their customers at face value. Regulated non-bank providers are also end users.</td>
</tr>
<tr>
<td>Integrators</td>
<td>Integrators develop custom applications that add value to the baseline features. They provide customer service, training and support to their users. Integrators are also end users.</td>
</tr>
<tr>
<td>Businesses</td>
<td>Businesses are end users of the FPN.</td>
</tr>
<tr>
<td>Persons</td>
<td>Persons are end users of the FPN.</td>
</tr>
</tbody>
</table>

### Enrollment

Enrollment is a one-time step and is not included in the end-to-end payment process. The enrollment process is freely accessible by all U.S. consumers and businesses and may be available from other geographic areas (e.g., Canada, Latin America) as determined by the FPN’s rules.

The purpose of enrollment is to allow entities to establish payment addresses in the Global Directory Service (GDS). The payment address functions as a digital wallet to hold, receive, and transfer Federal Reserve notes (Fed notes) for payment. The enrollment process is simple. The following graphic shows the overview of the process flow for the enrollment process.
Enrollment Available All Day, Every Day
The person enrolling in the FPN visits the enrollment page (e.g., fednotes.net/signup) and is asked to complete a basic enrollment form. During enrollment, persons (individuals, not businesses) establish a unique identity and token for authenticating to the FPN. Enrollment is freely available to persons within the supported geographic areas all day, every day.

Information Requested During Enrollment
In addition to providing basic personal information, such as name, address, etc., an end user can choose whether to authenticate to the system using a password, hardware key, or biometric token. The enrollment process binds the token chosen by the end user to the end user’s identity
and address in the GDS. The token can be a password, passphrase, or private key in a public-private key pair.

**Enrollment Token Security**

If an end user elects to use a password as a token, the enrollment form requires the password to be of a certain length and to use specified characters. As the person enters a proposed password, the enrollment form shows its strength. Passwords that do not meet the required criteria are not accepted. The end user is advised to keep the password private. An end user who elects to use a hardware key as a security token should also keep it private.

**Enrollment CAPTCHA**

The FPN’s technical design includes a completely automated public turing test to tell computers and humans apart (CAPTCHA). The purpose of the enrollment CAPTCHA is to allow humans to enroll in the FPN while making it difficult for machines to enroll. Each end user enrolling in the FPN is required to complete a CAPTCHA.

**Stakeholders Also Enroll in the FPN**

Stakeholders include the Federal Reserve, the Governing Organization, depository institutions, regulated non-bank providers, integrators, businesses, and individuals. The FPN’s design requires enrollment by all participants, including persons who perform responsibilities on behalf of Stakeholders. An authorized person performs the one-time enrollment on behalf of a Stakeholder. Each of the Stakeholders also enrolls in the FPN to perform the functions associated with their responsibilities. For example, a representative of Dunkin’ Donuts is required to enroll as an individual and also create a business profile for Dunkin’ Donuts to perform functions related to accepting Fed notes for payment. Similarly, all Stakeholders are required to have one or more authorized representatives manage the Stakeholder’s business and act on behalf of the business in performing the Stakeholder’s responsibilities. For security reasons, permissions in the FPN are associated with personal credentials even for persons performing functions on behalf of a Stakeholder.

**Enrollment in FPN is Business-Type Specific**

The information required for a business to enroll (e.g., business name, address, phone, web address, etc.) depends on the type of business as specified by the FPN’s rules. For example, a depository institution may provide enrollment information that differs from a retailer because of the depository institution's responsibilities as a distributor of Fed notes. The FPN’s design supports a tiered enrollment process, allowing for information to be incrementally gathered as it is needed to perform specific functions. For example, a business is required to provide a physical address and phone number but is not required to provide other documents (e.g., articles of incorporation, business license) until that information is needed as part of a request to increase the monetary value that the business can hold and transfer. The tiered enrollment process allows end users to get started with minimal information required and to provide additional information as needed.

---

as the need arises. The tiered enrollment process is also a key to achieving ubiquity by 2020 because it simplifies and minimizes the overall time and cost of enrollment for business.

**A Manager Acts on Behalf of a Business in Assigning Permission**
Unlike a person, a business does not have a credential associated with the business’ payment address. A business does not directly authenticate to the FPN. The person who enrolls the business becomes the manager of the business and receives the manager’s permission. The manager’s permission allows the manager to perform tasks within the FPN and to assign permissions to other persons to act on behalf of the business, including designating other managers. The permissions that a manager can assign are relevant to the payment address (e.g., business) and specific task (e.g., send, modify).

**Payment Address Customization, Payment Address Profile, and Contextual Data**
After enrollment, the FPN creates and assigns to the end user a permanent, globally unique, payment address in the Global Directory Service (GDS). The end user can choose to customize the payment address or add optional payment address aliases (e.g., email, cell phone, social media profile, deposit account, etc.). The customization of a payment address and a payment address alias are both a security and social sharing mechanism. The customized payment address provides the end user with a globally unique payment address that is easily shared publicly, including on social media sites, websites, billboards, business cards, marketing brochures, etc. The customized payment address is also a security mechanism because it is valueless outside the context of the FPN and reveals no sensitive information (e.g., payment card account number, checking account number).

The FPN’s technical design allows the end user to associate profile information (i.e., contextual data) with a payment address. For example, a person can provide, subject to the FPN’s privacy policy, payment address profile information after enrollment, including a phone number, a home address, a picture, and a related web address.

**Enhanced Privacy and Security for Persons Enrolling**
The security of the enrollment processes for persons is enhanced by providing support for a second factor authentication experience using Universal Second Factor (U2F) protocol and a passwordless authentication experience using Universal Authentication Framework (UAF) protocol. Both protocols are designed to provide stronger authentication with an open, scalable and interoperable set of mechanisms developed by the Fast Identity Online (FIDO) Alliance that use public key cryptography. The FIDO Alliance protocols are proposed standards that are gaining broad industry support, are easy to use, and enhance end user privacy and security.

The use of U2F protocol and certified devices (e.g., Yubikey) provide resistance against Man-in-the-Middle (MitM), phishing, session hijacking and malware attacks. The Google Chrome

---

8 See [Universal 2nd Factor (U2F) Overview](#) published 14 May, 2014 for additional information.
9 See [FIDO UAF Architectural Overview](#) published 08 December, 2014 for additional information.
10 See [FIDO Alliance.org specifications overview](#) for additional information.
browser was one of the first to build in support for FIDO Alliance protocols. The FIDO Alliance announced\textsuperscript{13} that it now has over 150 biometric and second-factor authentication products certified, including products by Ebay, Gemalto, Lenovo, LG Electronics, NTT Docomo, Qualcomm, RSA, Samsung, Sharp and Sony. NIST—the national program office for the National Strategies for Trusted Identities in Cyberspace\textsuperscript{14}, a White House Initiative to work collaboratively to improve privacy, security and convenience of online transactions—also joined the FIDO Alliance.\textsuperscript{15}

**Verifying a Primary Communication Channel at Enrollment**

The FPN’s technical design requires an end user to provide a primary communication channel (e.g., email, sms/text message) at enrollment. The primary communication channel must be verified before it is associated with the end user’s payment address in the GDS. The FPN verifies the primary communication channel by sending randomly generated information to the end user using the primary communication channel and requiring the end user to return to the FPN and enter the information.

**Establishing a Personal Identification Number**

The FPN’s technical design allows a person (individual, not business) to set up a personal identification number. The PIN has limited use and is only used to resume a session after an inactivity timeout.

**Persons and Businesses Have Limited Ability to Hold and Transfer Funds**

Both persons and businesses enrolled in the FPN have transfer limits, as specified by FPN rules, that restrict their ability to hold and transfer Fed notes until their identity is verified. Identity verification includes reviewing the accuracy of profile information submitted through sources outside of the FPN. For a person, outside sources may include government issued identification, employment information, pay stubs, tax returns, and credit bureaus. For a business, outside sources may include the Data Universal Numbering System (DUNS) and local, state and federal government agencies (e.g., Businesses Licensing, Division of Corporations). Acceptable outside source information is subject to FPN rules.

**Ongoing Efforts to Resist Threats and Attacks**

Security is an ongoing process and commitment. The enrollment and authentication processes are crucial to the security of the FPN. All that can be done should be done to defend, mitigate and resist known threats and attacks.

---


\textsuperscript{13} FIDO Alliance Announces Over 150 Biometric and Second-Factor Authentication Products Now Certified, FIDO Alliance.org, 4 April 2016.

\textsuperscript{14} National Strategy for Trusted Identities in Cyberspace (NSTIC), The National Institute of Standards and Technology, U.S. Department of Commerce.

\textsuperscript{15} NIST Joins the FIDO Alliance, NSTIC Notes, Updates from the National Program Office.
Authentication

Authentication is the first step of the iterative end-to-end payment process. When authenticating to the FPN, an enrolled end user identifies himself or herself and provides proof of identity using a credential with secret information only known to or in possession of the end user.

Varying Authentication Methods

The FPN’s technical design allows for authentication methods to vary; several use cases require strong second-factor authentication (e.g., biometric, hardware token). As a security mechanism, the FPN design also allows end user reauthentication to occur at various points in the iterative payment process. For example, an end user may be required to reauthenticate when proxying from a personal to a business payment address. Reauthentication can be required before an end user is permitted to sign and submit a payment order. For example, Jessica may authenticate to the FPN using a cryptographic hardware key and complete a transfer on her own behalf. She then proxies to her employer’s business payment address and fills out a payment order to pay Sysco Corporation for food delivery in the amount of $1579.89. Roger, the owner of business and manager of the business’s payment addresses has modified Jessica’s permissions and limits both the amount she can transfer and requires her to re-verify her credentials before she is allowed to sign and submit a payment order on behalf of the business.

The graphic below shows how the the FPN requires Jessica to reauthenticate using her hardware key before she can send a payment order. The send button on the left is dimmed because Jessica’s hardware key is not detected. When Jessica re-inserts the hardware key, the FPN detects the presence of the key and asks for her to sign the payment order. After she signs the payment order, the FPN determines that she is authorized to submit the payment order for the transfer to Sysco Corporation.

16 The FPN’s verification of a credential can be either simply checking to see that the hardware key is still present or requiring full reauthentication. The FPN’s verification of a hardware key on a payment order is an enhancement of the current implementation.
**Strong Second-Factor and Passwordless Authentication**

The FPN’s technical design supports the use of second-factor authentication with support for the U2F protocol using certified devices (e.g., hardware token). The U2F authentication experience augments security of existing password infrastructure by allowing the FPN to prompt the end user to present a second-factor device at any time\(^{17}\). The FPN’s design for the passwordless experience allows the end user a choice of local authentication mechanisms (e.g., swiping a finger, looking at a camera, or entering a PIN) to replace the password\(^{18}\). The FIDO Alliance protocols are proposed standards with broad industry adoption and are based on public key cryptography.

**Unsuccessful Authentication Attempts**

As a security mechanism, the FPN’s technical design requires end users to input a CAPTCHA after a specified number of unsuccessful authentication attempts and also supports setting a timeout before another authentication attempt is allowed (e.g., 30 seconds to hours).

**Token Reissueance**

The FPN’s technical design allows end users to change, renew or reissue the token. The FPN allows the end user to change a password or passphrase token using the end user’s primary communication channel verified during the enrollment process. The FPN’s design for reissuing a new token to replacing a lost or stolen hardware key requires the use of a secondary communication channel (e.g., text message) and a secondary second factor authentication method (e.g. one-time password).

**End User Authentication Using a Published Application**

Integrators use the API to provide value-added features to end users. Although the integrator provides value-added features, the integrator does not authenticate to the FPN on behalf of the end user. The FPN’s technical design requires integrators to use the OAuth 2.0 Authorization Framework\(^{19}\), a standard published by the Internet Engineering Task Force (IETF). A published application created by an integrator is issued a limited attribute access token, which is different from the end user’s authentication credential, when permission is granted to the published application by the end user. Separating the end user’s credentials from the published application’s access token adds a layer of protection to the authentication model.

**FPN Functions Available to Authenticated End Users**

End users are required to successfully authenticate to the FPN before being able to interact with the FPN. (See S.7.1 and S.10-End User/Provider Authentication.) End user interactions that require authentication include, but are not limited to, the following:

- Completing, signing, and submitting payment orders
- Viewing transfer history

---

\(^{17}\) Specifications Overview, FIDO Alliance.

\(^{18}\) Specifications Overview, FIDO Alliance.

\(^{19}\) The OAuth 2.0 Authorization Framework, Internet Engineering Task Force (IETF), October 2012.
Faster Payments Network Solution Proposal

- Adding, changing, or removing a verified payment address alias
- Adding optional information to a payment address profile
- Updating notification preferences
- Canceling a payment address
- Managing, adding, or removing devices and published application permissions
- Changing or updating credentials or tokens
- Creating a PIN or using a hardware token
- Enrolling a business

**FPN Allows Limited Non-Authenticated Interaction**

The FPN allows limited, non-authenticated interaction that may include, the following, as permitted by FPN rules:

- Browsing a directory of enrolled businesses and viewing a business’s publicly available profile information
- Viewing participation and privacy policy agreements and other applicable disclosures and notices
- Viewing help and frequently asked questions
- Viewing an end user’s publicly available profile information, if applicable
- Validating the authenticity of a Fed note by viewing the security features of the Fed note or by cryptographically validating the Fed note’s digital signature.

**Protecting Sensitive Information**

The FPN’s design allows persons to authenticate with a username without entering sensitive information (e.g., checking account number). The FPN’s design also allows persons to authenticate using a hardware key and public/private key pair to replace or enhance the username and password. The FPN’s design does not require persons to publically share payment address profile information.

**Payment Orders (includes Initiation & Payer Authorization)**

The payment order stage is also part of the iterative process in the payment life cycle where the end user provides specific instructions to the FPN for executing a transfer. The payment order stage consolidates the steps of initiation and payer authorization from the eight stage payment life cycle defined in the proposal template.

**Payers Authorize Transfers by Completing a Payment Order**

Payment orders allow a Payer to provide specific instructions to the FPN to execute a transfer. The payer must complete, sign and submit a payment order to the FPN to make a payment. The FPN executes the Payer’s instructions as provided on the payment order in real time, without

---

20 Canceling a payment address makes it and all of the payment address aliases unusable but does not delete the transfer history for that payment address.
human intervention or review, 24 hours a day, every day of the week; therefore, the Payer is accountable and solely responsible for the accuracy of information submitted on payment orders to the FPN. Transfers are final the moment they are completed by the FPN as specified by the Payer on the payment order. As a security mechanism, the FPN’s design for the processing of payment orders allows for push-only transfers that involve a national currency (e.g., USD). The FPN’s design does not permit a Payee to submit a payment order on behalf of the Payer (i.e., pull transfer).

**Optional Reauthentication for a Payment Order**

The FPN allows the manager of a business payment address to require reauthentication of a payment order for some transfers with specified qualities. For example, the manager of a business may require reauthentication using a second-factor token for transfers in excess of $1000.

**Internet-Connected Devices and Applications Supported**

End users complete, sign and submit payment orders using supported Internet-connected devices and/or published applications. Supported Internet-connected devices include desktop computers, tablets, smartphones and feature phones. Supported applications include web browsers and other applications developed by integrators and approved for publication to end users by the Governing Organization (see G.1).

End users can complete payment orders in many ways using various devices, channels and supported applications. In general, the end user authenticates to the FPN to complete a payment order.

**Fields on the Default Payment Order**

The FPN’s technical design specifies the following fields as part of a default payment order: (a) the national currency code, (b) the transfer amount, (c) the currency types included in the transfer (e.g., open-loop or closed-loop), (d) the text of a message to be included with the transfer, (e) privacy setting for the transfer, and (f) a hash of any cryptographic token used to sign the payment order.

**Payment Order with Support for Invitations**

The FPN’s technical design permits enrolled entities to submit a payment order for a recipient that does not yet have a payment address in the GDS. When a payment order is submitted for a person that does not yet have a payment address in the GDS, the notification sent to the person is referred to as an invitation.

Invitations can be sent to email addresses, cell phone numbers, and profiles on supported social media sites (e.g., Facebook, Twitter). When the FPN determines that the payment is to a destination not in the GDS, the FPN partially processes, then pauses, the payment order to notify the recipient using the method specified on the payment order. The FPN’s design specifies that

---

21 Requires integration into the mobile carrier network to achieve appropriate security.
the Payer can cancel an invitation any time before the FPN completes the transfer to the recipient. An invitation cannot be cancelled by the Payer after the recipient enrolls in the FPN and the FPN completes the transfer. The FPN’s design for invitations drives viral growth and is key to achieving widespread adoption by 2020. The graphic below shows the process flow for a payment order with support for invitations.

**Payment Order Supports Transfers by ACH**

The FPN’s design allows entities to transfer funds via ACH to accounts that entities hold with a depository institution. The FPN’s rules specify that the holder of an account at a depository institution must first prove that the entity is named on the account before a payment address alias can be created for the account in the GDS.
The FPN’s use of a payment address alias for an account at a depository institution is a security mechanism and can provide knowledge of the identity of the end user. This security mechanism allows the account’s owner to make deposits, but it also protects the account and account number from unauthorized use (see S.9.2). The FPN’s integration with the ACH allows Fed notes to be deposited to accounts with a depository institution that is connected to the ACH network.

**Payment Orders with Multiple Currencies (and Multiple Issuers)**

The FPN’s technical design supports a multi-currency and multi-issuer architecture that enables any of the ISO 4217 standard currencies; however, each currency is to be issued by a financial institution (i.e., central bank or commercial bank) before it can be active on the FPN. A currency that is active on the FPN is also referred to as a national currency (i.e., USD, EUR) and is either open loop (i.e., national currency) or closed loop (i.e., brand cash).

**National Currency Issued by Financial Institutions in Standard Denominations**

Open-loop currency is a national currency issued by a Central Bank in standard denominations (e.g., $.01 to $100) and is permitted or restricted on the FPN as determined by the governance model (i.e., applicable rules, regulations, laws). The graphic below shows the face of a $100 Fed note on the FPN.

![USD $100 National Currency](image)

**National Currency Personalization or Co-Branding**

National currency can be personalized or co-branded. Personalization and co-branding means that the design and/or theme of the Fed notes are temporality changed from the default design.
For example, the design and theme can be personalized to support a special occasion (e.g., birthday, wedding, graduation). The Payer can personalize the design by selecting from a library of designs available like choosing a greeting card. After the design is selected and purchased from the library, it can be applied to the Fed notes and sent to the Payee. The following graphic shows the face of $1 Fed note personalized with happy birthday.

Co-branding is similar to personalization but is performed by businesses, and the design applied to the Fed notes is a design by the business related to their brand. For example, T-mobile may run a campaign offering those that purchase a phone cash back on the purchase. Rather than sending a prepaid card to the purchaser for the cash back, T-Mobile creates a design that features the T-Mobile name and logo. To send the cash back, T-Mobile applies the design to the Fed notes and sends them to the Payee. In this way, T-Mobile is delivering the cash back using the FPN and is also benefited by being able to place their name and logo on the Fed notes the Payee receives. The FPN’s design allows for personalization and co-branding to be a value-added service and represents a potential revenue opportunity for the Federal Reserve, Department of the Treasury, or GO.

**Cross-border Payments**
The FPN’s technical design allows for conversion from one currency to another as necessary for cross-border payments by: 1) separating the conversion process from the transfer process for cross-border payments, 2) allowing the Payer to determine the currency to transfer to the Payee,
3) allowing the Payee to receive the currency sent by the Payer, and 4) allowing the Payee to convert the currency as desired and with any number of conversion exchange providers offering currency exchange services.

For example, John is a U.S. citizen living in Mexico. John and his brother Kevin are the owners of a small bike shop in Alpine, Utah. Each month Kevin sends John $500 for his portion of the profits from the bike shop. Kevin logs into his bank and purchases $500 in Fed notes on the FPN. Kevin takes possession of the Fed notes. He completes, signs and submits a payment order to transfer $500 to his brother, John. John receives the transfer, converts the funds to Mexican pesos, and deposits them in his account at Banorte.

**Foreign Currency Conversion**

The FPN’s design allows end users to purchase a national currency (e.g., EUR) using another national currency (e.g., USD) using the website or a published application. The currency exchange provider presents a custom dialog to the purchaser that displays the fees for the exchange and the amount of the converted currency the purchaser will receive. The purchaser can view multiple currency exchange providers to find the best exchange rate. The FPN’s design allows all currency exchange providers (e.g., depository institutions and non-bank providers) to compete to provide currency exchange services.

The FPN’s technical design supports currency exchange for the following use cases: person to person, person to business, and business to business. For example, a person holding dollars could exchange with another person holding euros.

The FPN’s design protects both the sender and receiver in the currency exchange process from disclosing sensitive information to complete the exchange.

**Closed-loop Value Issued by Businesses**

Closed-loop is value issued by a business in standard denominations (e.g., $.01 to $100) and is restricted as determined by the issuer and FPN rules. The Issuer of the closed-loop value may
apply various limits including (a) expiration dates, (b) the total amount that can be held by a payment address, (c) the types of payment addresses that can hold the closed-loop value (e.g., person or business), (d) whether or not the closed-loop value is transferable to other payment addresses, (e) the amounts that can be redeemed in a single transfer to a payment address, and (f) payment addresses that can redeem the closed-loop value in exchange for goods and services.

Closed-loop value is also referred to as brand cash. The FPN’s technical design identifies the following on the face of each closed-loop note: (a) the name of the Issuer of the closed-loop note (e.g., Best Buy), (b) the value of each closed-loop note (e.g., $1), (c) the designer of the closed-loop note, (d) the locations where the closed-loop note may be redeemed for goods and services (e.g., Best Buy), (e) any limits associated with the closed-loop (e.g., expiration, transferability), and (f) an appropriate name that indicates the purpose of the closed-loop note (e.g., gift, loyalty, rewards, promotional, humanitarian, or welfare). The graphic below shows $100 MCX rewards. The face of the closed-loop note shows the issuer, the redemption locations, the holder and other information.

**USD $100 MCX Rewards**

The current holder of this cash can send it to pay for products and services. These businesses accept MCX Rewards:

- Costco Wholesale
- Sam’s Club
- Target
- Walmart

<table>
<thead>
<tr>
<th>Serial No.</th>
<th>Value</th>
<th>Holder</th>
<th>Provider</th>
<th>Designer</th>
<th>Transferable</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>W001-T99E-339D-C2E8</td>
<td>USD $100 (One Hundred United States dollars)</td>
<td>Bradley Wilkes</td>
<td>Merchant Customer Exchange</td>
<td>Agency Fusion</td>
<td>Yes</td>
<td>Never</td>
</tr>
</tbody>
</table>

**Issuance of Closed-loop Value is a Value-Added Feature**

The FPN’s technical design allows the governing organization (GO) to utilize a vetting process to either grant or restrict a payment address from having the ability to issue closed-loop currency. Thus, the ability for a business to issue a closed-loop currency is a value-added feature of the
Faster Payments Network Solution Proposal

FPN. The FPN also enables the Issuer of closed-loop value to determine participants in the closed-loop network. Participants in the closed-loop network may be assigned different roles and permissions as a member of the closed-loop network. For example, a common role is “redemption.” As members of a closed-loop network, redeemers are the payment addresses where closed-loop value is exchanged for goods and services. Another common role in a closed-loop network is “distributor.” The closed-loop network also has a role for “settlor.” The settlor is the payment address that exchanges redeemed closed-loop value for payment in a national currency. The FPN’s ability to enable businesses to issue closed-loop value is a key to achieving widespread adoption and also presents a potential revenue-generating opportunity for the GO.

Administrator Configures Default Capabilities
The FPN allows an administrator to set the default currency for each payment address. The currency default is “inherited” by a newly created payment address. The FPN allows the payment address owner to modify the defaults. For example, a business may determine that it would like to accept MXN in addition to USD for payment.

Intelligent Redemption of Closed-Loop Value
The FPN’s technical design also defines a liquidity algorithm that operates at the payment order stage. The liquidity algorithm is sophisticated logic and represents the core mechanism executing transfers on the FPN. The liquidity algorithm intelligently assists the Payer with selecting currency types when completing a payment order.

The liquidity algorithm is aware of the context of the Payer within the FPN. When the Payer selects a destination for a transfer, the liquidity algorithm’s logic determines the applicable use case (e.g., P2P, P2B). The liquidity algorithm also receives parameters for the Payer that include the Payer’s payment address settings and preferences, national currencies held by the Payer, types of closed-loop value held by the Payer, and the limiting parameters of the closed-loop value held by the Payer (e.g., expiration dates, total amounts). The liquidity algorithm also receives parameters for the Payee that include the national currencies accepted by the Payee, the Payee’s payment address settings, and the Payee’s memberships in closed-loop networks.

The liquidity algorithm analyzes the various parameters it receives to return information needed to intelligently construct a payment order that includes an ordered list of the currency types and amounts of currency available for this specific payment order. The ordered currency list is arranged by liquidity with the least liquid currency types at the top of the list (e.g., closed-loop value with limits) and the most liquid (e.g., Fed notes) at the bottom. The FPN’s technical design defaults to applying the total amount of the payment order to the ordered currency list from top to bottom—using the least liquid currency before the use of more liquid currency. The Payer can adjust the order of the currency on the payment order before signing and submitting the payment order.

The graphic below shows the payment order dialog without the ordered currency list displayed. When the Payer clicks “choose cash types,” the ordered currency list is displayed. For the payment order in the graphic, the Payer would redeem $80 of closed-loop value before transferring $45 in Fed notes.
The liquidity algorithm also incorporates rules, regulations and laws applicable to transfers to ensure that transfers on the FPN are executed appropriately.

**Payment Order Workflow**

A unique and important aspect of the FPN’s technical design is the association of one or more automated workflows with a payment order when it is submitted by the Payer to the FPN. Because workflows are automated, the end user is not usually even aware of the workflow process.

The workflow can vary in complexity depending on the requirements for the payment order. Workflows are flexible and manage the entire sequence of steps associated with executing a transfer, including pausing a transfer, resuming a transfer, making change for a Fed note, making change for closed-loop value, sending notifications when a transfer is in progress or complete, returning closed-loop value to the issuer, expiring closed-loop value, creation of payment codes, etc.
The transfer of $.01 from John to Jane is a simple transfer; however, even this simple transfer has many steps in the workflow that depend on variables for the FPN to consider when executing the transfer. For example, if John wants to send a $.01 to Jane but he holds only $.05, then the FPN makes change for the $.05 before transferring the $.01. The process of making change requires additional steps in the workflow.

While the end user does not need to be aware of the workflow process, all the steps in the workflow are permanently recorded and available for review by the end user and the stakeholders in the transfer. The graphic below shows the steps for a $1 transfer from Bradley Wilkes to Jacob Christensen.

Payee Customized Payment Order
The FPN’s design enables a Payee to customize the payment order for the Payer. Using a customized payment order, the Payee may require the Payer to provide additional information before the payment order can be signed and submitted. The FPN’s design allows the required fields of a payment order to be specified by the Payee. For example, the payee may add an account number field to the payment order and specify whether it is required or optional. The FPN’s ability to enable the Payee to customize the payment order assists the Payee in gathering

Payment dialog customization is an enhancement to the current implementation.
required information for the payment. Customized payment orders are not designed to be a replacement for a Payee’s invoicing process; rather the design is to assist the Payee in connecting payments to other information (e.g., invoices).

**Two Payer Signatures on a Payment Order**

The FPN’s technical design supports requiring an approver and/or two payer signatures before the payment order can be submitted to the FPN. In the example below, a large non-profit organization requires two signatures on each payment order before it can be submitted to the FPN.

In the example below, a large non-profit organization requires two signatures on each payment order before it can be submitted to the FPN.

---

**Disclosure of End User Fees**

The FPN’s design allows transfers to occur without transfer fees for targeted use cases. The FPN’s design also supports transfer fees for certain transfers. For example, a retailer (e.g., Target) can set up an automatic deposit to an account at a depository institution. The depository institution discloses the fee for the deposit, and the automatic deposit is enabled. In another example, a depository institution has a deposit fee for persons making a deposit. The amount of the deposit fee is disclosed to the person at the time of the deposit.

**Receipt (Clearing, Settlement, and Notification)**

The final step of the iterative, end-to-end payment process is receipt. The FPN’s receipt stage includes the clearing and settlement stages from the eight-stage payments life cycle defined in the proposal template and adds the notification step.

---

23 Two Payer Signatures is an enhancement to the current implementation.
Receipt Overview
In the receipt stage, the FPN puts the Payee in possession of the Fed notes as instructed and authorized by the Payer, the holder of the Fed notes. The moment the FPN updates the possession attribute on the Fed notes, the Payee is in possession of good funds issued by the central bank. The FPN's design specifies that the update of the possession attribute occurs in real time when the Payer submits the payment order. If the FPN is not able to complete the update of the possession attribute, then an error message is displayed to the Payer who then knows immediately that the transfer was not successful. If the FPN is able to complete the update of the possession attribute, then a confirmation of successful payment is displayed to the Payer. The FPN’s design does not require the Payee to be authenticated to receive a transfer. The graphic below shows the process flow for the receipt stage.
Contextual Data included with the Payment
The FPN’s design allows the Payer to include a message with the payment to the Payee. The design also allows the Payee to reply to the message included with payment from the Payer. Other contextual data is available with the payment, including the payment type, the start date and time, end date and time, status, participants (i.e., Payer, Payee and stakeholders) and visibility of the transfer (e.g., public or private).
Concurrence of Clearing and Settlement
The FPN’s technical design mimics the use of physical Fed notes for payments. Therefore, similar to using physical Fed notes for payment, clearing and settlement of digital Fed notes occurs concurrently with the update to the possession attribute on the Fed notes. The FPN’s design to use Fed notes for transfer eliminates the lag between availability of funds and settlement and also credit and liquidity risk.

Notification to the Payee Follows Receipt
Receipt means the possession attribute of the Fed notes has been updated by the FPN and shows the payment address of the Payee as the holder. The receipt step includes the FPN’s sending notification to both the Payer and Payee through verified communication channels (e.g., email, SMS/text message, social media profile post, certified app) that the transfer is complete and final. Notification immediately follows receipt. It is included in the receipt stage because it only occurs for the Payee when a transfer is complete. If a Payer attempts a transfer that fails, only the Payer is notified of the failure (not the Payee). A Payee may receive notification of a completed transfer in more than one media channel simultaneously. For example, Joe may receive notification of payment from Jane as an email message and as a private message on an instant messaging service (e.g., Twitter).

Records for Each Payment
The FPN creates and stores a record of each transfer, including contextual data in the transfer history that is accessible to the Payer, Payee and other stakeholders that are a party to the transfer (e.g., Issuer of closed-loop value).

Optional Payment Codes
The FPN’s technical design specifies an optional step that allows the Payee to validate the payment before it is received. The FPN allows the Payee to require the Payer to present a unique payment code to the Payee for validation before the transfer can be complete. The FPN’s use of payment codes is similar to a preauthorization. The graphic below shows the process flow for the receipt stage with payment codes.
Short Payment Codes or Long Tokens

A payment code can be represented as a short code (e.g., four to five randomly generated numeric characters) or a longer token. The FPN’s technical design specifies the random generation of a one-time short code or token after the Payer has completed, signed and submitted a payment order to the FPN.

Payment Code Security Mechanism

Payment codes have a security mechanism that limits the validation of the short code or token to a single payment address or to many payment addresses arranged into a hierarchy with the root or parent of the hierarchy specifying a single name (e.g., Walmart, Target, Chevron) for all payment addresses in the hierarchy.

Payment Codes for up to the Amount of Funds Held

The FPN’s technical design allows a Payer to generate a payment code provided the Payer is in possession of the funds sufficient to cover the amount preauthorized by the payment code. However, the generation of the payment code does not freeze funds held by the Payer. For example, Joe holds $1 in Fed notes. Joe can generate a $1 payment code for Target and a $1 payment code for Walmart. Joe cannot generate a payment code for $1.01 to either Target or Walmart because $1.01 exceeds the amount of funds held by Joe.

Payment Code Validation on a First-Come, First-Served Basis

The FPN’s technical design allows for payment codes to be validated on a first-come, first-served basis and for the currency underlying the payment code to be transferred only once, regardless of the number of payment codes generated for the underlying currency.

For example, Joe holds only $1 in Fed notes but he has generated two $1 payment codes—one for Target and one for Walmart. Joe stops by Walmart on the way home and buys a pack of gum.
for $.79. He provides his payment code to the cashier, and she validates the payment. Walmart receives $.79 for Joe’s purchase of gum. Joe stops in Target to purchase a second pack of gum for $.79. Joe provides the Target cashier with the Target payment code, but the cashier receives an insufficient funds error when she attempts to validate the payment code. Joe no longer holds sufficient funds to cover the purchase; consequently, Joe must return the gum or produce another form of payment.

The FPN’s technical design does not have a concept of overdraft. The FPN’s technical design limits the transfer of funds to funds currently held by the Payer, including closed-loop value.

**Modifications to Payment Codes Are Immediate**

The FPN’s technical design allows the Payer, after a payment code has been generated but before it has been presented to the payee, to (a) cancel the payment code, (b) skip the payment code and instruct the FPN to perform the transfer immediately, or (c) adjust the expiration of the payment code. Option (b) above allows the Payer to skip a payment code and direct the FPN to complete the transfer immediately. Payees can disable the Payer’s ability to skip the payment code. All the Payer’s modifications to a payment code are updated in real time.

**Payment Address Chains**

A collection of payment addresses arranged into a hierarchy is called a chain. When payment addresses are arranged in a chain, the FPN’s technical design allows the Payer to specify the name provided at the root level of the hierarchy on the payment order, but the resulting payment code can be validated once by any one payment address in the chain before the payment code expires or is canceled.

**Options for Communicating Payment Codes**

Payment codes can be transmitted by the Payer to the Payee in a variety of methods, including transmission by Near Field Communication (NFC), Bluetooth, barcode, Quick Response Code (QR code), SMS/text message, email message, or manually provided (e.g., read over the phone, in a face-to-face setting).

**Validating Payment Codes**

The FPN’s technical design allows payment codes to be validated by the Payee using a web application or certified point-of-sale (e.g., Micros, Square, Clover) system that has an application developed by an integrator using the API. The Payee can validate the payment code for up to the maximum value authorized by the Payer. Upon validation by the Payee, the FPN completes the transfer for the amount validated, provided the Payer is holding sufficient funds to complete the transfer. If the Payer does not hold sufficient funds, the payment code validation process will immediately return an insufficient funds error message to the Payee. The Payee can also experience other error codes, including payment code canceled, over the amount authorized, service unavailable, etc.

---

24 Transmission of payment codes by NFC, Bluetooth, barcode and QR code are enhancements to the current implementation.
Payment Codes in the Real World
For example, Costa Vida, a restaurant chain with eight corporate locations in Utah, has their cashiers validate the payment using a short payment code and a Micros POS. The person making a purchase at Costa Vida and using the FPN for payment authenticates to the FPN and specifies Costa Vida as the Payee on the payment order. The person estimates the amount of the purchase at Costa Vida and enters that estimate on the payment order. The person then signs and submits the payment order. The FPN displays the short payment code to the purchaser. After ordering, the purchaser presents the short payment code to the cashier for payment. After entering the purchaser’s order into the POS, the cashier validates the payment code for the exact amount of the purchase. The purchase is complete. Costa Vida enjoys immediate final payment and the purchaser enjoys a delicious smothered burrito.

Return of Payment Received in Error
The FPN’s design allows a recipient to return a payment received in error. The Payer may also request the Payee return a payment sent in error. However, a Payer cannot reverse or cancel a payment made in error without the Payee’s knowledge and cooperation.

Reconciliation
Reconciliation is an optional step of the end-to-end payment process.

The FPN stores a record of each transfer in the end user’s transfer history. Transfer history information is available to the Payer, Payee and other stakeholders in the transfer to support post-transfer evaluation. The FPN retains the transfer history according to data retention rules. The graphic below shows a transfer history report.
The FPN’s technical design supports the reconciliation step by downloading transfer information in standard formats (e.g., CSV, JSON,) for various systems that perform reconciliation (e.g., Quickbooks, Quicken, Mint, Sage 50). The download of information to support reconciliation does not require the download of sensitive information.

In addition to downloading transfer information, the FPN provides various reports to support reconciliation. For example, in addition to transfer history, the FPN provides a received and receivable report (see graphic below) and a distribution and redemption report. The FPN’s design enables access to information in standard formats to allow analysis using a wide range of programming languages, analysis tools, and applications.
As a security mechanism, the FPN makes downloads and reports available only to authenticated end users and stakeholders with access permissions.

**Approval by the Payer’s Provider**

The FPN’s technical design mimics the use of physical Fed notes for payment; therefore, similar to using physical Fed notes for payment, approval by the Payer’s provider is not necessary unless the provider is acting as the Payer. The FPN’s use of Fed notes eliminates credit and liquidity risk and ensures that all transfers are conducted in good funds.

The FPN processes all payment orders upon submission. The transfers associated with processing a payment order are immediate and become final when the FPN updates the possession attribute on the Fed notes from the Payer to the Payee.

**Part A, Section 2: Use Case Description**

The previous section, *Part A, Section 1: Solution Description*, describes what the FPN does for each stage of the payment process life cycle. This section describes what the FPN does that is unique at each stage of the life cycle for each of the four supported use cases.
While there are functions unique to each supported use case as described below, most of the FPN’s functional design is consistent for all four supported use cases. For example, the message flow, contextual data capability, use of the liquidity algorithm, use of automated workflow, roles and responsibilities of stakeholders, and other functions are consistent with the description in the previous section.

**Person-to-Person**

<table>
<thead>
<tr>
<th>Life Cycle</th>
<th>Unique Functions?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment (one-time)</td>
<td>Y</td>
<td>Only persons (individuals, not businesses) establish an identity and credential at enrollment for authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The recipient of a payment may be responding to an invitation and is not yet enrolled in the FPN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The person may be required to establish a credential using strong second-factor authentication to perform some functions on behalf of a business.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Y</td>
<td>Only persons (individuals, not businesses) authenticate to the FPN.</td>
</tr>
<tr>
<td>Payment Order</td>
<td>Y</td>
<td>A payment order can initiate an invitation for a transfer to a payment address not yet in the GDS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Invitations can be sent to email addresses, cellphone numbers, and/or supported social media profiles.</td>
</tr>
<tr>
<td>Receipt</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Reconciliation (optional)</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>

**Person-to-Business**

<table>
<thead>
<tr>
<th>Life Cycle</th>
<th>Unique Functions?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment (one-time)</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Payment</td>
<td>Y</td>
<td>The FPN allows payment order fields to be customized by Payees (i.e., businesses)</td>
</tr>
</tbody>
</table>
### Person-to-Business Use Case

<table>
<thead>
<tr>
<th>Life Cycle</th>
<th>Unique Functions?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td></td>
<td>therefore the payment order may have additional required fields for the Payer.</td>
</tr>
<tr>
<td>Receipt</td>
<td><strong>Y</strong></td>
<td>The FPN allows Payees (i.e. businesses) to require Payers to provide payment codes to be used by the Payees to validate payments. When payment codes are required, the payment code is generated and displayed to the Payer after the payment order is submitted but before transfer is received by the Payee.</td>
</tr>
<tr>
<td>Reconciliation</td>
<td><strong>N</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- Enrollment (one-time) **N**
- Authentication **Y**
- Payment Order **Y**
- Receipt **N**
- Reconciliation (optional) **N**

### Business-to-Person

<table>
<thead>
<tr>
<th>Life Cycle</th>
<th>Unique Functions?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment (one-time)</td>
<td><strong>N</strong></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td><strong>Y</strong></td>
<td>A person with permissions proxies to the business’s payment address after successful authentication. The FPN allows businesses to require persons to authenticate with strong second-factor authentication before being able to proxy to the business’s payment address. The FPN allows requiring re-authentication based on a person's permissions and/or the amount to be transferred on the payment order.</td>
</tr>
<tr>
<td>Payment Order</td>
<td><strong>Y</strong></td>
<td>The FPN allows the payment order to be configured to require two signatures before it can be submitted to the FPN. The FPN sends an invitation for payment orders that specify transfer to payment addresses not yet added to the GDS. Invitations can be sent to email addresses, cellphone numbers, and/or supported social media profiles.</td>
</tr>
<tr>
<td>Receipt</td>
<td><strong>N</strong></td>
<td></td>
</tr>
<tr>
<td>Reconciliation</td>
<td><strong>N</strong></td>
<td></td>
</tr>
</tbody>
</table>
Business-to-Business

<table>
<thead>
<tr>
<th>Life Cycle</th>
<th>Unique Functions?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment (one-time)</td>
<td>N</td>
<td>A person with permissions proxies to the business’s payment address after successful authentication. The FPN allows businesses to require persons to authenticate with strong second-factor authentication before being able to proxy to the business’s payment address. The FPN allows requiring re-authentication based on a person’s permissions and/or the amount to be transferred on the payment order.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Y</td>
<td>The FPN allows the payment order to be configured to require two signatures before it can be submitted to the FPN.</td>
</tr>
<tr>
<td>Receipt</td>
<td>Y</td>
<td>The FPN allows Payees (i.e. businesses) to require Payers to provide payment codes to be used by Payees to validate payments. When payment codes are required, the payment code is generated and displayed to the Payer after the payment order is submitted but before transfer is received by the Payee.</td>
</tr>
</tbody>
</table>

Reconciliation (optional) N

Part A, Section 3: Use Case by Effectiveness Criteria

The table below summarizes the FPN for use case by effectiveness criteria.

<table>
<thead>
<tr>
<th>Use Case by Effectiveness Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation (part of payment order)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Faster Payments Network Solution Proposal

| Authentication | U.2 | Y | Y | Y | Y |
| U.3 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |
| S.10 | Y | Y | Y | Y |

| Payer Authorization (part of payment order) | U.2 | Y | Y | Y | Y |
| U.3 | Y | Y | Y | Y |
| S.2 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |

| Approval by the Payer’s provider (not required on FPN unless provider is Payer) | S.3 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |
| F.1 | Y | Y | Y | Y |
| F.5 | Y | Y | Y | Y |

| Clearing (part of Receipt stage) | E.4 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |
| F.2 | Y | Y | Y | Y |

| Receipt | U.1 | Y | Y | Y | Y |
| U.2 | Y | Y | Y | Y |
| U.3 | Y | Y | Y | Y |
| U.6 | Y | Y | Y | Y |
| S.5 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |
| F.3 | Y | Y | Y | Y |
| F.5 | Y | Y | Y | Y |

| Settlement (part of Receipt stage) | S.4 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |
| F.4 | Y | Y | Y | Y |

| Reconciliation (*optional external to FPN) | U.3 | Y | Y | Y | Y |
| E.7 | Y | Y | Y | Y |
| S.5 | Y | Y | Y | Y |
| S.6 | Y | Y | Y | Y |
| S.7 | Y | Y | Y | Y |
| S.9 | Y | Y | Y | Y |
PART B: BUSINESS CONSIDERATIONS

The technology to support the FPN has been in development since January of 2009 and operating in local markets since 2011. The section below entitled “Technical Features in the Current Open Source Implementation” provides a detailed list of developed, fully tested and implemented features for the FPN. The section that follows entitled “Technical Features at Implementation of the FPN” provides a list of features that will be added before implementation in 2018. All existing features and existing code plus new features and new code will be fully tested for implementation. Development and testing are continual and iterative processes that ensure quality and security of the FPN. The Governing Organization, working with key vendors, should ensure that all features and code are fully tested in a staging environment that mimics production before being released.

The current open source version is interoperable with existing payment systems, including the ACH network, the payment card networks, the bill pay networks, and other payment networks.

Interoperability

**Interoperable with the ACH Network**

The FPN’s technical design interoperates with the ACH network, providing access to accounts at depository institutions that are members of the ACH network. The use of the ACH network to move funds from the FPN to an account at a depository institution using the ACH is completed at the speed of the ACH network and is not immediate. However, depository institutions that interface their core systems directly to the FPN using the API will receive transfers immediately and be able to make immediate deposits to customer accounts.

**Interoperable with Payment Card Networks**

Although the technology in the current implementation is designed to interoperate with payment card networks, no cardholder data is stored by the current implementation. The proposer does not suggest the FPN directly interoperate with the payment card networks; rather, interoperability will be achieved by integrators that use the API to work within both the payment card networks and the FPN. The graphic below provides an example of how interoperability is achieved with the payment card networks.
Interoperability with the payment card networks is indirect and will be driven by integrators that develop Internet (e.g., shopping carts), mobile and digital wallet applications.

**Interoperable with Other Payment Networks**

The FPN is also interoperable with the other networks (e.g., Bill Pay, TCH’s faster payments initiative, Dwolla, Ripple) using the API.

**Implementation Timeline**

The proposer recommends that the work to implement the FPN begin immediately following the publication of the final paper. The Implementation Timeline table below suggests a high-level implementation plan. The implementation timeline presented below is also referred to in Part C, Section 2, Efficiency. Milestones are indicated with the checkered flag. A more detailed implementation plan is needed to support the many hundreds of tasks that need to be coordinated to implement the FPN by 2018.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Delivery Date</th>
<th>Owner(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faster Payments Network Final Proposal Assessment</td>
<td>Q4-2016</td>
<td>QIAT, FPTF</td>
</tr>
<tr>
<td>Task Description</td>
<td>Delivery Date</td>
<td>Owner(s)</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Proposal Adopted</td>
<td>Q1-2017</td>
<td>FPTF, Fed</td>
</tr>
<tr>
<td>Final Paper Published</td>
<td>Q1-2017</td>
<td>FPTF, Fed</td>
</tr>
<tr>
<td>Charter the Governing Organization (GO)</td>
<td>Q1-2017</td>
<td>Fed, SC, FPTF</td>
</tr>
<tr>
<td>Grandfather FPTF into GO membership (no membership fee due until 2020)</td>
<td>Q1-2017</td>
<td>Fed, FPTF, GO</td>
</tr>
<tr>
<td>Recruit and hire the Implementation Team (IT)</td>
<td>Q1-2017</td>
<td>Fed, GO</td>
</tr>
<tr>
<td>Hire executives and staff for the GO</td>
<td>Q1-2017</td>
<td>Fed, GO</td>
</tr>
<tr>
<td>Establish process and criteria for vendor selection (e.g., data centers, hosting, hardware, software applications security, etc.)</td>
<td>Q1-2017</td>
<td>Fed, GO</td>
</tr>
<tr>
<td>Start FPN awareness campaign (ongoing)</td>
<td>Q2-2017</td>
<td>Fed, GO</td>
</tr>
<tr>
<td>Formal Draft of FPN Rules</td>
<td>Q2-2017</td>
<td>Fed, GO</td>
</tr>
<tr>
<td>Add details to high-level implementation plan</td>
<td>Q2-2017</td>
<td>GO, IT</td>
</tr>
<tr>
<td>Optional: Convert open source application stack to proprietary application stack that offers indemnity (e.g., IBM).</td>
<td>Q2-2017</td>
<td>GO, Fed, Vendor</td>
</tr>
<tr>
<td>Obtain commitments from Depository Institutions (DI’s) to distribute Federal Reserve notes for FPN (ongoing – identify those DI’s willing to stand in for the Fed as Issuers until statutory approval)</td>
<td>Q2-2017</td>
<td>GO, Fed</td>
</tr>
<tr>
<td>Get commitment from retailers to integrate POS systems to FPN (ongoing with focus on largest retailers first to achieve ubiquity)</td>
<td>Q2-2017</td>
<td>GO, Fed</td>
</tr>
<tr>
<td>Get brand cash issuance commitments from retailers (ongoing)</td>
<td>Q2-2017</td>
<td>GO</td>
</tr>
<tr>
<td>Get commitments from federal, state and local governments and agencies to replace less efficient payments (e.g., checks and payment cards) with FPN</td>
<td>Q2-2017</td>
<td>GO, Fed</td>
</tr>
<tr>
<td>Obtain consensus vote on FPN rules by membership</td>
<td>Q3-2017</td>
<td>GO</td>
</tr>
<tr>
<td>Obtain, configure and deploy hardware and software for FPN sandbox for integrators to begin integration</td>
<td>Q3-2017</td>
<td>GO, Vendors</td>
</tr>
</tbody>
</table>
**Implementation Timeline**

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Delivery Date</th>
<th>Owner(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin a campaign to increase awareness of FPN for integrators (ongoing)</td>
<td>Q3-2017</td>
<td>Fed, GO</td>
</tr>
<tr>
<td>Begin a campaign to encourage depository institutions to interface core systems directly to FPN.</td>
<td>Q4-2017</td>
<td>GO, Fed</td>
</tr>
<tr>
<td>Build and test the Network Operations Center</td>
<td>Q2-2018</td>
<td>GO, IT, Vendors</td>
</tr>
<tr>
<td>Conduct large-scale tests on production</td>
<td>Q2-2018</td>
<td>GO, IT, Vendors</td>
</tr>
<tr>
<td>Launch Faster Payments Network (initial implementation)</td>
<td>Q3-2018</td>
<td>Fed, GO, IT, Vendors</td>
</tr>
<tr>
<td>Continuous Improvement of FPN (ongoing)</td>
<td>Q3-2018</td>
<td>GO, Vendors</td>
</tr>
<tr>
<td>Begin launch awareness campaign</td>
<td>Q3-2018</td>
<td>GO, Fed</td>
</tr>
<tr>
<td>FPN achieves ubiquity (Congratulations!)</td>
<td>Q4-2020</td>
<td>All</td>
</tr>
</tbody>
</table>

**Technical Features in the Current Open Source Implementation**

The following is a list of features that are available in the current open source version of the implementation and are expected to be included in the initial implementation of the FPN.

- Enrollment for persons in the U.S. and other countries as permitted by the rules
- Enrollment for businesses in the U.S. including federal, state and local governments, retailers, etc., and for businesses in other countries as permitted by the rules
- Enrollment for depository institutions in the U.S. and in other countries as permitted by the rules
- Enrollment and support for national currency issuance by central banks in other countries as permitted by the rules
- ACH network integration and support for transfer of funds to accounts held at depository institutions
- Support for businesses and governments to issue closed-loop value (e.g., gift, loyalty, rewards, promotional, humanitarian, and welfare programs) with offers and campaign tracking (Businesses administer their own closed-loop networks with appropriate distribution and redemption agreements for network participants.)
- Support for sharing data using open data sharing formats, including a live web page (e.g., HTML5), Atom, JSON, and streaming
- Open API using OAuth2 for integrators
• Features to support customized branding by depository institutions and regulated non-bank providers using domain name aliasing and themes
• Reports, including transfer history, page groups, provider liabilities, distribution and redemption, received, and receivable
• Support for businesses to have payment addresses with public information published in the Global Directory Service
• Automatic sweep to deposit account with a fixed fee per sweep
• Administrative features include:
  o Payment address management
  o Enrollment management
  o Transfer analysis

**Technical Features at Implementation of FPN**

The following is a list of features that will be added prior to implementation of the FPN in 2018:

• Two-factor authentication with support for one-time passwords (OTP), Universal 2nd Factor (U2F) protocol and Universal Authentication Framework (UAF) protocol
• Enhancements to the API to allow a Payee to customize the payment order dialog and specify the required fields
• One-time password delivery by SMS/text message
• Analytics dashboard
• Automatic sweep to deposit account with fixed fee per sweep plus ad valorem (taxes)
• Multiple signatures on payment orders for businesses
• Scheduled payments for a date in the future
• User interface and functional improvements as needed to support implementation and scale

**Value Proposition and Competition**

The proposal defines each stakeholder and the stakeholder’s roles and responsibilities. The value propositions of the stakeholder do not vary by stage of the payment lifecycle (e.g., enrollment, authentication, payment order, receipt, reconciliation). The section below presents the value propositions for each stakeholder to adopt the FPN.

**Value Proposition for the Federal Reserve**

The Federal Reserve has the roles of regulator, issuer of the Fed notes and accountability and financial responsibility in the case of failure of the Governing Organization. The Federal Reserve also controls the Internet domain where the Fed notes are published and where the Global Directory Service is made available. The value propositions for the Federal Reserve to adopt the FPN are as follows:

1. The Federal Reserve is in a unique position to see that the FPN is offered equitably for all U.S. consumers and businesses, including depository institutions, with public policy goals of speed, ubiquity, safety and efficiency receiving priority over commercial interests.
2. The Federal Reserve can expect to receive “full recovery of costs over the long run”\textsuperscript{25} by directing savings from printing, transportation and destrulations costs of digital Fed note issuance into the operation of the FPN.

3. The Federal Reserve as regulator, issuer and controller of the Internet domain will "promote integrity of the payments system,"\textsuperscript{26} and instill public confidence.

4. Adoption by the Federal Reserve will “avoid undue delay in the development and implementation of the service.”\textsuperscript{27} Depository institutions are not likely to implement the service voluntarily without the Federal Reserve because the FPN is viewed as a threat to payment card revenues.

5. The Federal Reserve will continue to recognize seigniorage for Fed notes issued using the FPN.

6. The Federal Reserve’s role as issuer of Fed notes with distribution equitably across all depository institutions also makes it possible for depository institutions of all sizes and incumbency to compete with each other for consumer and business deposits.

7. The Federal Reserve does not compete with depository institutions and regulated non-bank providers in providing deposit accounts to consumers or businesses.

The table below summaries the value propositions above by use case for the Federal Reserve. The table shows if the value proposition is true (Y) or not (N) for Federal Reserve for the targeted use case as numbered above.

<table>
<thead>
<tr>
<th>Value Proposition by Use Case for Federal Reserve</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
</tbody>
</table>

**Value Proposition for Depository Institutions**

Depository institutions have the roles and responsibilities as distributors and depositories of Fed notes. The Fed notes are ordered by depository institutions from the Federal Reserve and held for transfer on demand to their customers. Depository institutions with integration of their core

\textsuperscript{25} Strategies for Improving the US Payment System, Board of Governors of the Federal Reserve System, by Financial Services Policy Committee, January 26, 2015, p. 56.

\textsuperscript{26} Strategies for Improving the US Payment System, Board of Governors of the Federal Reserve System, by Financial Services Policy Committee, January 26, 2015, p. 56.

\textsuperscript{27} Strategies for Improving the US Payment System, Board of Governors of the Federal Reserve System, by Financial Services Policy Committee, January 26, 2015, p. 56.
systems using the API are able to accept Fed notes for immediate credit to a customer's account. The value propositions for depository institutions to adopt the FPN are as follows:

1. To compete with other depository institutions in providing services to their customers, including distribution and deposit of digital Fed notes.
2. Depository institutions are able to determine the fee charged to the customer for depositing Fed notes to an account.
3. Depository institutions using the API and their own branded applications are able to offer the baseline services and value-added services to their customers.
4. Depository institutions have no inter-provider credit or liquidity risk when accepting Fed notes for deposit.
5. The FPN does not place additional regulatory burden on the depository institutions for participating in the FPN.

The table below summarizes the value propositions above by use case for Depository Institutions. The table shows if the value proposition is true (Y) or not (N) for Depository Institutions for the targeted use case.

<table>
<thead>
<tr>
<th>Value Proposition by Use Case for Depository Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

**Value Proposition for Regulated Non-Bank Providers**

Regulated non-bank providers act as depositories of Fed notes, providers of the baseline features and value-added services to their customers. Although regulated non-bank providers, like depository institutions, offer depository services to their customers, because they do not have accounts with the Federal Reserve, they do not have the role and responsibilities of distributing Fed notes. The value propositions for regulated non-bank providers adopting the FPN include the following:

1. Regulated non-bank providers are able to determine the fee charged to the customers for depositing Fed notes to an account.
2. Regulated non-bank providers using the API in their own branded applications are able to offer the baseline services and value-added services to their customers.
3. Regulated non-bank providers have no inter-provider credit or liquidity risk when accepting Fed notes for deposit from their customers.
4. The FPN does not place additional regulatory burden on the regulated non-bank providers for participating in the FPN.

The table below summarizes the value propositions above by use case for regulated non-bank providers. The table shows if the value proposition is true (Y) or not (N) for regulated non-bank providers for the targeted use case.
Value Proposition by Use Case for Regulated Non-Bank Providers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Value Proposition for Businesses

Businesses are entities or end users that use the FPN. The value propositions for businesses to adopt the FPN include the following:

1. Businesses may enroll in the FPN without paying an enrollment fee.
2. Businesses may enroll in the FPN without established credit.
3. Businesses may cancel enrollment in the FPN at any time without paying a cancellation fee.
4. Businesses do not pay a transfer fee when a customer chooses to pay with Fed notes.
5. Businesses receipt of payment in Fed notes is immediate, final and in good funds.
6. Businesses deposit Fed notes with FRS member depository institutions.
7. Businesses do not receive sensitive customer information that they are required to protect as part of the payment from a customer.
8. Businesses are not required to maintain special or dedicated equipment (e.g., EMV equipped terminal) to accept transfers from customers.
9. Businesses also utilize the Global Directory Service to issue their own brand cash to offer incentives (e.g., rewards, loyalty) to customers who pay with Fed notes.
10. Businesses use the API to integrate their POS systems, allowing full analytics for all transfers.
11. Businesses do not “make change” when accepting Fed notes transfers from customers; all transfers are for exact amounts.
12. Businesses do not need to count Fed notes at the end of the day or at the end of a cashier's shift.
13. Businesses uniquely customize their payment address to help customers know where to send the payment. (e.g., fednotes.net/walmart)
14. Businesses use their payment address in advertising.
15. Businesses use brand cash and offers for promotion and advertising.
16. Enrolling a single business in the system is simple and can be completed in as little as five minutes.
17. Businesses can safely and securely send and receive payments in Fed notes both in person and remotely, with the ability to track and account for every payment.

The following table summaries the value propositions above by use case for businesses. The table shows if each value proposition (as numbered above) applies (Y) or not (N) to businesses for the targeted use case.
Value Proposition by Use Case for Businesses

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>8</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>10</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>11</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>12</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>13</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>14</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>15</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>16</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>17</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

Value Proposition for Persons

Persons are end users of the FPN. The value propositions for persons adopting the FPN include the following:

1. Persons enroll in the system without paying an enrollment fee.
2. Persons can cancel enrollment at any time without paying a cancellation fee.
3. Persons send or receive Fed notes without paying transfer fees.
4. Persons send or receive Fed notes without sharing or receiving sensitive information (e.g., debit card number, checking account number).
5. Persons create and verify optional payment address aliases for their social media profiles, email addresses, and cell phones to help others route transfers to them.
6. Persons can create a unique customized payment address and share it.
7. Persons control the information that is displayed on their payment address profile.
8. Persons control their own credentials.
9. Persons hold and transfer Fed notes (i.e., open-loop value), closed-loop value issued by businesses, and other currencies with a single payment address.
10. The FPN is designed to suggest that users redeem closed-loop value they hold before using Fed notes (i.e., open-loop value) when Persons are purchasing from businesses that redeem closed-loop value they hold.
11. Persons can deposit Fed notes to FRS member depository institutions or regulated non-bank providers.
12. Persons make purchases from businesses that accept Fed notes.
13. Persons are holding Fed notes issued by the Federal Reserve.
14. Persons can view a record of every transfer in their transfer history.
15. Persons access the system with freely available applications (e.g., web browsers) and common Internet-connected devices (e.g., mobile phone, tablet).
16. Persons with poor credit history or no credit history can enroll in the system.

The table below summaries the value propositions above by use case for Persons. The table shows if the value proposition (as numbered above) applies (Y) or not (N) to Persons for the targeted use case.

<table>
<thead>
<tr>
<th>Value Proposition by Use Case for Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
</tbody>
</table>

Value Proposition for Integrators

Integrators are software developers, third-party processors, third-party service providers, technology providers, billers, depository institutions, regulated non-bank providers, businesses, etc. The Federal Reserve’s issuance of Fed notes, coupled with the FPN’s technical design, expands the payments ecosystem by making digital Fed notes globally accessible in many countries, in any language, with various devices and through many channels. The value propositions for integrators to adopt the FPN include the following:

1. The FPN’s technical design provides integrators various integration points (e.g., data streams, activity feeds, webhooks, domain name aliasing, themes, and the API)
2. Integration is achieved using current Internet standards (see E.4, S.6.3-4) and technologies.
3. Integration provides information for analytics and tracking of offers and campaigns that utilize brand cash.
4. Integration allows integrators to provide value-added services.
5. Integration allows integrators to customize the end user’s experience.
6. Integration allows integrators to differentiate themselves and offer services under their brand.

The table below summarizes the value propositions above by use case for integrators. The table shows if each value proposition is true (Y) or not (N) for the integrators in the targeted use case.

<table>
<thead>
<tr>
<th>Value Proposition by Use Case for Integrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

**Integration Effort**

The FPN provides various points of integration that are available to the stakeholders and seeks to maintain existing relationships between stakeholders. Integration points vary in their ease of use, with activity feeds as the simplest form of integration and webhooks and the API on the more complicated end of the range.

**Points of Integration**

Points of integration are set up, managed and controlled by either the end user (e.g., activity feeds, webhooks, domain name alias) or by the Governing Organization that manages the API and certification process for integrators developing applications. The points of integration do not vary by use case; however, the FPN’s design offers domain name aliasing as a point of integration for approved stakeholders (i.e. depository institutions). Domain name aliasing allows other stakeholders (e.g., Wells Fargo) to have a portion of their domain name (e.g., fpn.wellsfargo.com) resolve to the FPN (e.g., fednotes.net). In addition to allowing stakeholders to provide access to their customers using a URL their customers recognize (e.g., fpn.wellsfargo.com), it also allows the stakeholder to provide access under its own brand and its own color theme. Although domain name aliasing is configured by an approved entity (e.g., Wells Fargo), the feature would need to be administratively activated by the GO before it is available for configuration.

The API has function calls to support enrollment, authentication using OAuth2 for a published application, payment orders, receipt, and reconciliation. The activity feeds and webhooks have points of integration to support payment orders, receipt and reconciliation. The following table shows the points of integration that are available at each stage of the payments life cycle.

<table>
<thead>
<tr>
<th>Points of Integration Available by Payment Life Cycle Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points of Integration</td>
</tr>
<tr>
<td>Activity Feeds†</td>
</tr>
<tr>
<td>Webhooks</td>
</tr>
</tbody>
</table>
The FPN’s technical design specifies a central, Internet-accessible, domain (e.g., fednotes.net) with varying points of integration and multiple integration methods (e.g., API, activity feeds, and webhooks) for integrators. Each integration method has a point of integration, also known as an endpoint.

The points of integration for each method vary based on the authenticated user and/or the application requirements. For example, the table below illustrates the points of integration for each type of activity feed created by the Clinton Campaign to allow the Clinton Campaign to track and disclose donations received.

<table>
<thead>
<tr>
<th>Activity Feed Method</th>
<th>Example Point of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live web page</td>
<td><a href="https://fednotes.net/clintoncampaign/feed/1/">https://fednotes.net/clintoncampaign/feed/1/</a></td>
</tr>
<tr>
<td>Atom (similar to RSS)</td>
<td><a href="https://fednotes.net/clintoncampaign/feed/1/">https://fednotes.net/clintoncampaign/feed/1/</a></td>
</tr>
<tr>
<td>JSON Snapshot</td>
<td><a href="https://fednotes.net/clintoncampaign/feed/1/">https://fednotes.net/clintoncampaign/feed/1/</a></td>
</tr>
<tr>
<td>Streaming</td>
<td><a href="https://stream.fednotes.net/feed_chunked/7770156854/1/">https://stream.fednotes.net/feed_chunked/7770156854/1/</a></td>
</tr>
<tr>
<td>Widget28</td>
<td>&lt;iframe src=&quot;https://fednotes.net/clintoncampaign/feed/1/&quot;&gt;&lt;/iframe&gt;</td>
</tr>
</tbody>
</table>

Webhooks specifically allow an entity to specify the endpoint for an application. For example, suppose the Trump Campaign has built an application and wants to receive notifications for each type of event that occurs for the Trump Campaign payment address. The Trump Campaign configures the endpoint using a webhook (e.g., www.donaldjtrump.com/FPN/event). In addition to allowing the entity to specify the point of integration, webhooks allow the entity to specify the type of information that the FPN will send to the endpoint. Webhooks also notify the listening application immediately when events occur.

In addition to the points of integration listed above, the current open source implementation has an open and fully documented API29 that details 33 functions calls that specify endpoints for integrators. The API was first released in December 2013 and as of March 17, 2016, has been

---

28 Widgets are designed to be added to web page to display certain transfer information.
29 See wingcash.com/api to view the full API documentation.
updated 18 times. As updates are made to the FPN, corresponding changes and enhancements will be made in the API. Integrators with published applications that use the API will be required to periodically recertify their application to ensure compatibility with the API.

The FPN’s technical design does not require specific points of integration for stakeholders for the targeted use cases, but it does provide points of integration across a spectrum of options, from enabling simple data streams to a full-function API. The table below summarize the the points of integration available to integrators (i.e., stakeholders) by use case.

<table>
<thead>
<tr>
<th>Points of Integration available to Integrators by Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
</tr>
<tr>
<td>Live web page</td>
</tr>
<tr>
<td>Atom</td>
</tr>
<tr>
<td>JSON</td>
</tr>
<tr>
<td>Widget</td>
</tr>
<tr>
<td>Webhook</td>
</tr>
<tr>
<td>Full API</td>
</tr>
</tbody>
</table>

The FPN’s technical design allows the entity to specify whether endpoints should be public or private. Private points of integration are secured by issuance of a private key that is controlled by the entity enabling the endpoint. The FPN allows the entity enabling the endpoint to share the key, change the key, or completely remove the endpoint. The purpose of issuing a private key is to secure the endpoint and enable only certain applications to access the information provided by the endpoint.

**Relative Effort Required for Integration by Stakeholder**

The FPN’s implementation of an open API makes it possible for integrators to develop value-added services directly as their resources permit without being dependent on other parties, including the Governing Organization or the Federal Reserve.

Integration times may vary by stakeholder due to factors outside the control of the proposer, including the skills and experience of the integrator, the complexity of the integration chosen by the integrator, and the availability of resources to the integrator. The author’s small team completed an integration with the Micros POS in approximately three weeks. The relative effort required for integration is estimated to take 1-10 days for an activity feed, 10-180 days for a webhook, and 90-180+ days using the full API.

**Business Relationships Between Stakeholders**

The FPN’s design seeks to maintain the business relationships that exist between stakeholders. For example, depository institutions are members of the Federal Reserve System and order Federal bank notes from the Federal Reserve; with the introduction of the FPN, depository institutions will be transferred digital Fed notes electronically rather than receiving printed notes by armored car services.
Depository institutions also maintain the relationships they have with their customers (e.g., provide customers with Fed notes when requested and accept Fed notes for deposit). Regulated non-bank providers maintain the relationships they have with their customers (e.g., cash advances, loans, check cashing). Businesses also maintain the relationships they have with their depository institutions and their customers. The FPN is a platform to enable transfers between all parties enrolled without requiring modification of existing relationships between participants. The FPN’s design is neutral and non-exclusionary; it doesn’t prevent or prohibit participants from forming relationships.

**PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA**

The FPN meets the standards of ubiquity, efficiency, safety and security, and speed set forth by the Faster Payment Task Force. The FPN also has a solid legal framework and rules for governance as outlined in this section of the Faster Payments Network solution proposal.

**Part C, Section 1: Ubiquity**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Section &amp; Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.1, Accessibility</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.2, Usability</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.3, Predictability</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.4, Contextual Data</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.5, Cross-Border Functionality</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.6, Applicability to Multiple Use Cases</td>
<td>✔</td>
</tr>
</tbody>
</table>

**U.1, Accessibility**

Accessibility means the Solution should enable any entity (e.g., consumer, business, government agency, or financial institution) to initiate and/or receive payments to/from any entity consistent with applicable legal restrictions (see L.1.4, Compliance with U.S. Law on page 146).

**U.1.1, Support for Payment Accounts**

The Solution should facilitate payments to/from all types of payment accounts based in the United States (U.S.) held at all depository institutions and regulated non-bank providers.

The FPN’s technical design facilitates payments to and from all types of payment accounts by allowing entities to create links between the entities payment address and deposit accounts at all depository institutions and regulated non-bank providers. Once these links are established, the
entity can use the link to transfer funds to all types of deposit accounts (e.g., checking, savings, money market, etc) through the ACH network.

The FPN’s technical design optionally allows providers to connect directly with and integrate their core systems to the GDS using the API. Providers integrating directly with the GDS make it possible for entities to transfer directly to/from deposit accounts with the provider in real-time.

View a demonstration of how providers are integrated with the GDS to facilitate payments to/from all types of payment accounts.

**U.1.2, Payer Confidence**

The Solution should demonstrate how all entities choosing to use the Solution can be sure that their payments can reach any and all Payees.

Entities using the FPN have the following assurances that their payments reached all Payees:

- The FPN allows a Payer to use a known payment address (e.g., email, cell phone, social media profile, token, etc.) for the Payee when submitting a payment order.
- The FPN presents payment confirmation information to the Payer with information showing that processing of the signed payment order submitted by the Payer has been completed. (In the case where the Payer’s signed payment order is submitted through an integrator using the API, then the FPN returns payment confirmation information through the third-party application.)
- The Payer is able to visually confirm that the system has updated the possession attribute of the Fed notes involved in the transfer and that the Fed notes now show the Payee’s Primary Payment Address. (In the default case where the transfer is set to private, the Payer could alternatively visit the transfer history to see the list of Fed notes the Payee holds.)
- The Payer and Payee receive notification through established communication channels (e.g., email, text message, notification on smart phone, etc.) that the transfer is complete and the system has placed the Payee in possession of the Fed notes(s).

- Visually confirm the possession attribute of Fed notes has been updated.
- Receive notification of payment via established communication channel.
- Use a known payment address to find a Payee and make a payment.

**U.1.3, Support for Multi-Currency Payments**

The Solution should have the ability to support multi-currency payments.
The FPN’s technical design supports payments in all applicable currencies defined on the ISO 4217 currency code specification (the “Standard Currencies”). The FPN supports multi-currency payments by allowing other Central Banks and/or providers to also issue national currencies to the GDS denominated in any one of the Standard Currencies. The FPN’s technical design allows for the representation and transfer of value in fixed units (e.g., $1.00 MXN or $1.00 USD) rather than the transfer of value using debits and credits (i.e., double-entry accounting). It is the fixed-units transfer mechanism coupled with the use of the Internet standard for URLs that makes it simple to support all currencies within the FPN and to avoid certain issues associated with building a network based on double-entry accounting.

View how the FPN supports multiple currencies by allowing the following:

- A central bank being approved to issue national currency.
- A central bank creating and distributing national currency to depository institutions.
- A depository institution transferring banknotes to customers.

**U.1.4, Address Needs of Unbanked and Underserved**

The Solution should effectively address the needs of the unbanked or underserved to affordably send or receive payments. For example, it should support the ability to make payments to/from regulated non-bank provider and/or explicitly promote financial inclusion in the payments Solution.

The FPN’s technical design includes the following features to enable the unbanked or underserved to send or receive affordable payments:

- The FPN allows the unbanked or underserved to freely obtain payment addresses in the GDS.
- The FPN allows the unbanked and underserved to send and receive immediate payments without transfer fees.
- The FPN encourages financial inclusion by allowing the unbanked and underbanked to select providers, including depository institutions, that enable value added features (e.g., deposit account, line of credit) available to them.

View a demonstration of entities using the system to do the following:

---

30 The FPN limits enrollment of other central banks or financial institutions unless done so according to regulation, law and under an approved participation agreement.
31 The rules will specify what information is required for basic enrollment and the total amount a basic payment address can hold.
View a demonstration of entities using the system to do the following:

- Freely obtaining a Payment Address.
- Sending and receiving immediate payments without transfer fees.
- Selecting from a provider, opening an account, and making a deposit.

A person considered unbanked opens an account with a depository institution before being able to deposit Fed notes.

U.1.5, Credible Plan for Widespread Adoption

The Solution should provide a credible plan for achieving widespread adoption. The plan should demonstrate credibility by showing that the Solution is technically feasible for providers to adopt it and explaining how providers are motivated to participate and to make the Solution available to end users.

U.1.5.1, Achieve Widespread Adoption by 2020

The FPN will achieve widespread adoption by 2020 by executing a top-down adoption plan as follows:

1. Implement the FPN in mid-2018.
2. Obtain commitments and implementation timelines from the top 50 retailers to adopt the FPN.
3. Secure integration, distribution and depository services commitments from the top 50 depository institutions that provide services to consumers and businesses.
4. Obtain commitment from federal, state and local government agencies to modernize distribution of social program payments, including a commitment from United States Post Office to provide physical to digital exchange services to the underbanked and unbanked.
5. Obtain an integration commitment and timeline from the top five mobile wallet application providers (e.g., Apple, Samsung, Google, PayPal, CurrentC)

The FPN has important attributes to encourage end users to adopt the system. These attributes include the following:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible</td>
<td>Enrollment in the FPN can be completed in minutes and is freely available to all U.S. consumers and businesses.</td>
</tr>
<tr>
<td>Free Transfers</td>
<td>Transfers on the FPN have no transfer fees for the supported use cases.</td>
</tr>
<tr>
<td>Secure</td>
<td>The FPN operates on a “push” basis and does not require the sharing or exchange of sensitive information between Payer and Payee.</td>
</tr>
</tbody>
</table>
### Important Attributes Driving Adoption

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate</td>
<td>The FPN performs all transfers immediately after the payment order is received.</td>
</tr>
<tr>
<td>Final</td>
<td>Transfers on the FPN are irrevocable.</td>
</tr>
<tr>
<td>Credible</td>
<td>Transfers are completed with Fed notes authoritatively issued by the Federal Reserve.</td>
</tr>
<tr>
<td>Open</td>
<td>The FPN has an open API allowing integrators to provide the baseline features and value-added features.</td>
</tr>
<tr>
<td>Social Media</td>
<td>The FPN mimics many of the attributes that have allowed social media to quickly gain ubiquity (i.e., creation and sharing of custom payment addresses, creation and management of profiles, etc.)</td>
</tr>
<tr>
<td>Closed-Loop</td>
<td>The FPN enables businesses utilizing the GDS to provide gift, loyalty, rewards, promotional, welfare and humanitarian programs.</td>
</tr>
</tbody>
</table>

**U.1.5.2 Implementation and Launch by 2018**

To achieve widespread adoption by 2020, the FPN’s implementation should occur in mid-2018. Delays in implementation may also impact the ability to achieve widespread adoption by 2020. The author recommends that the work on the widespread adoption plan presented here, including obtaining commitments from retailers, depository institutions, mobile wallet providers and government agencies, begin in early 2017.

**U.1.5.3 Adoption by the Top 50 Retailers**

The FPN is particularly appealing for the top 50 retailers to adopt; however, because of their size and the complexity of their point-of-sale systems, discussions about integrating with the FPN should begin in early 2017, so the Governing Organization can obtain commitments with a timeline from these organizations. The timing for obtaining such commitments may be just right. Many of the large retailers demonstrated discontent with the cost of accepting payment cards.\(^{32}\)

**U.1.5.3.1, Closed-Loop Value Drives Adoption by the Retailer’s Customers**

The meetings with the top 50 retailers should include a discussion about their issuing closed-loop value (i.e., brand cash) and how the retailer will use closed-loop value to provide an incentive to customers to adopt and pay with the FPN.

Today one way retailers pay for rewards and loyalty is through the payment card networks in the form of an interchange fee. Closed-loop value is a mechanism that allows retailers to offer closed-loop loyalty and rewards directly to their customers for paying in Fed notes through the FPN. Retailers benefit when customers pay through the FPN because it eliminates the cost of interchange and the cost of returned checks.

---

Retailers can use a simple formula to determine the amount of loyalty and rewards they can provide to their FPN customers by computing the average discount for acceptance of payment cards, divided by cost of goods sold as a percent of sales. For example, if a retailer pays an average payment card discount rate of 2% and the retailer’s average COGS is 80%, then

\[ \frac{.02}{.80} = .025 \]

The equation shows that the retailer can offer customers paying with the FPN 2.5% in closed-loop value (i.e., loyalty) for all purchases without experiencing any additional cost. Arguably, however, the retailer has an improved financial position even after offering the discount because the FPN eliminates chargeback risk and reduces the exposure of sensitive customer information (i.e., payment card information) that could be stolen. Furthermore, the closed-loop value provided represents a future liability for the retailer that is realized when it is redeemed by the customer, while interchange expense is a current liability.

Closed-loop value is not limited to rewards and loyalty. It can be used in print, billboard, television, radio and social media marketing and advertising campaigns.

The author has used closed-loop value in various campaigns. The first campaign was two days after releasing the brand cash feature in production. The campaign included a simple email invitation to customers of Mountain West Burrito. The customers included in the campaign had participated in a giveaway on Facebook where the merchant offered a free burrito a week for 52 weeks. The offer was for $3 of brand cash, which was equivalent to the price of chips and salsa. Within 40 minutes, the offer had a nine percent acceptance rate. The first day after the distribution of the offer, 5.3 percent of those that had accepted the offer had redeemed the brand cash. Within 7 days after the distribution of the offer, fourteen percent of those that had accepted the offer had redeemed it. Because the merchant was integrated at the point-of-sale, analysis was performed for the redemptions. The merchant experienced nearly $4 in sales for each $1 distributed by the offer.

Another successful campaign distributed a total of $126 of free brand cash in a single offer from 17 merchants representing 27 different redemption locations. The offer was promoted on a blog with cross posts to social media sites. The offer was limited so that it could only be accepted by the first 750 people on a first-come, first-served basis. The offer was sold out in less than 40 minutes, distributing a total brand cash value of $96,500. The graph below shows the offer’s performance by redemption ratio for each of the participating merchants. Eight of the 17 merchants experienced redemption rates over five percent, and two of the merchants experienced redemption rates of 11 percent or more.
Awareness, Social Media Style

Because the FPN is operated from an Internet domain, it can benefit from the same promotional mechanisms that helped social media achieve ubiquity. Just as businesses place links to their social media profiles on their website homepages to encourage likes and followers, businesses will likewise place links to advertisements and promotional materials that refer to their profile on the FPN. While businesses do this to help customers find their profile on the FPN, it also serves as a powerful no-cost branding and awareness mechanism to help the FPN achieve widespread adoption.

U.1.5.4, Adoption by the Top 50 Depository Institutions

The FPN’s design allows participation by all depository institutions that have accounts with the Federal Reserve to achieve widespread adoption by 2020. The FPN is an attractive method of payment for depository institutions to adopt and offer to their customers.

Branding Opportunities for Depository Institutions

The FPN preserves the brand of the depository institution in the following important ways:

- The depository institution can offer customers a fully branded experience with value-added services by adding features in their existing applications using the API.
- The depository institution’s customers that create a link between a payment address alias and an account at the depository institution have an image with the depository institution’s name and logo.
- The depository institution can use domain name aliasing to provide its customers access to the baseline features at a domain controlled by the depository institution.

The FPN’s design allows customers with a linked account at a depository institution to choose to display the depository institution's name and logo on the customer’s own profile page.

Fees for Distribution or Deposit of Fed Notes

The FPN’s design also supports customers paying a fee to their depository institutions for the deposit or distribution of Fed notes. Depository institutions can use those fees to recover integration costs and contribute to profits.
Reduction in Costs and Elimination of Risk

The adoption of the FPN by depository institutions allows them to provide Fed notes to their customers at a lower cost and with reduced risk as compared with using physical Fed notes. For example, using the FPN, the Federal Reserve can deliver Fed notes to the depository institution immediately and without transportation costs. Furthermore, the FPN does not require the depository institution’s employees to handle and count Fed notes on the FPN. The FPN’s design also allows the depository institutions to manage the amount of Fed notes on hand and just as easily return Fed notes to the Federal Reserve.

Elimination of Credit and Liquidity Risk

The FPN’s use of Fed notes eliminates credit and liquidity risk for deposits received from customers and for transfers between depository institutions.

U.1.5.5, Adoption by Federal, State, and Local Governments

Benefit Payments for Social Programs

The FPN begins to achieve widespread adoption when federal, state, and local governments replace higher cost, less secure methods of distributing benefits for social programs (e.g., SNAP, WIC, TANF, SSI) with Fed notes using the FPN. The FPN also enables the use of closed-loop value for distribution of benefits, providing the social program administrator a high degree of control on redemption of the closed-loop value. For example, closed-loop value can be distributed to a program recipient that can be used exclusively at specific grocery stores. Furthermore, closed-loop value can be made non-transferable so that redemption can be performed only by the intended recipient. The FPN also allows the distribution of benefits directly to a third-party payee on behalf of a program recipient, saving distribution costs associated with checks, payment cards, and late payment fees. Social program administrators can completely automate the distribution of benefits using the API. The FPN also allows the social program administrator to verify the intended recipient or the recipient’s payee.

Announcing a government agency’s intention to switch from less efficient payment options to the FPN with instructions about how retailers can prepare themselves for the change will also drive adoption by retailers and the providers of point-of-sale systems.

Accessible by U.S. Consumers and Business

The FPN’s accessibility supports its adoption by federal, state and local governments. The FPN is freely accessible by U.S. consumers and businesses using the Internet and supported devices. In the U.S., 71% of mobile phones are smartphones (Internet-enabled). The FPN is also available to the unbanked and underbanked and does not require a credit score or credit history to participate.

Reduced Acceptance Cost

The FPN eliminates acceptance costs for merchants accepting payments on behalf of social program recipients. Adoption by government agencies decreases costs incurred with other payment methods (e.g., printing and mailing of checks or the production and distribution of secure payment cards). For example, the Social Security Administration (SSA) issues more than 600,000 checks to retired expatriates every year. Adoption by the SSA will eliminate postage and fees related to distributing checks to expatriates. Adoption by the IRS will decrease the amount the IRS pays in fees when persons pay their taxes in Fed notes using the FPN. Other common
government payments, including grants, loans and tax refunds issued, can be sent on the FPN. These are just a few examples of how the FPN will benefit government agencies and promote adoption.

**Attractive Method for Government Agencies to Receive Payments**

The FPN is an attractive method for government agencies to receive payments from consumers and businesses. Unlike other payment networks that may include sensitive information (e.g., payment card information) that the Payee has to protect, the FPN does not require the sharing or transmission of the Payer’s sensitive information. Consequently, government agencies do not have an obligation to protect information associated with receipt of payments.

The FPN also reduces the cost of compliance (e.g., PCI) and risk of theft or loss of sensitive information. The FPN also does not require government agencies adopting the FPN to purchase, maintain and upgrade dedicated point-of-sale equipment (e.g., payment card terminal) to receive a payment. Government agencies can also use payment address alias features of the FPN to collect payments remotely 24 hours a day for the use of parks, campgrounds, parking, parking tickets, etc.

**Adoption by Department of the Treasury**

The FPN has no print, transportation, or destruction costs for Fed notes. The table below shows the 2016 Federal Reserve Note Print Order with total print cost of $726 million for the printing of 7.6 billion Fed notes (an average cost of 9½ cents per note).

<table>
<thead>
<tr>
<th>Bill</th>
<th>Number Printed (in millions)</th>
<th>Total Value (in millions)</th>
<th>Cost/Bill</th>
<th>Total Cost (in millions)</th>
<th>Seigniorage (in millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1</td>
<td>2,425.60</td>
<td>$2,425.60</td>
<td>0.055</td>
<td>$133.41</td>
<td>$2,292.19</td>
</tr>
<tr>
<td>$2</td>
<td>179.20</td>
<td>$358.40</td>
<td>0.055</td>
<td>$9.86</td>
<td>$348.54</td>
</tr>
<tr>
<td>$5</td>
<td>819.20</td>
<td>$4,096.00</td>
<td>0.109</td>
<td>$89.29</td>
<td>$4,006.71</td>
</tr>
<tr>
<td>$10</td>
<td>480.00</td>
<td>$4,800.00</td>
<td>0.099</td>
<td>$47.52</td>
<td>$4,752.48</td>
</tr>
<tr>
<td>$20</td>
<td>1,939.20</td>
<td>$38,784.00</td>
<td>0.106</td>
<td>$205.56</td>
<td>$38,578.44</td>
</tr>
<tr>
<td>$50</td>
<td>224.00</td>
<td>$11,200.00</td>
<td>0.106</td>
<td>$23.74</td>
<td>$11,176.26</td>
</tr>
<tr>
<td>$100</td>
<td>1,516.80</td>
<td>$151,680.00</td>
<td>0.143</td>
<td>$216.90</td>
<td>$151,463.10</td>
</tr>
<tr>
<td>Totals</td>
<td>7,584.00</td>
<td>$213,334.00</td>
<td></td>
<td>$726.28</td>
<td>$212,617.72</td>
</tr>
</tbody>
</table>

**Adoption by the United States Post Office**

While adoption by depository institutions is important, depository institutions do not have retail locations that reach all consumers, especially the unbanked. The United States Postal Service (Postal Service) has physical locations in every American neighborhood. The author believes the Postal Service can help the FPN reach ubiquity by providing financial services to the underbanked and unbanked that utilize the FPN. For example, in May 2015 the Postal Service

---

published “The Road Ahead for Postal Financial Services.” The report includes opportunities for the Postal Service to provide postal financial services. The report presents the financial products the Postal Service may be permitted to provide under current law, and these include electronic money transfer, check cashing, and bill payment. The Postal Service recognizes that adoption of new financial services will help provide the physical link to the new digital economy.

The Postal Service also wants to modernize money orders. The closed-loop features of the FPN present an opportunity for the Postal Service to modernize money orders and international remittances with automated settlement upon redemption in Fed notes.

U.1.5.6, Integration by Mobile Wallet App Providers

Obtaining commitments with an integration timeline from the top providers of mobile wallets (e.g., Apple, Google, PayPal, and Samsung) is a key to achieving widespread adoption. Consumers are most likely to adopt the FPN when it can be trusted and is convenient, easy to use and available on the devices that consumers have.

U.1.6, Interoperability Across Networks

If the Solution includes multiple operators or networks, it should have a credible plan to achieve interoperability across these entities. The plan should demonstrate credibility by showing that a payment initiated through one operator/network/provider can be received by a user served by another operator/network/provider.

The FPN’s technical design allows it to interoperate with the following networks: payment card networks, ACH network, social media networks, email systems, mobile carrier networks, and personal contact applications and directories. The FPN achieves interoperability with these networks by following a general principle for interoperability using the GDS as the interoperability mechanism.

The FPN’s GDS adheres to the principle of allowing participants to control their own entries in the GDS. Participants have incentives to keep the entries in the GDS current so that transfers will be completed immediately. When network interoperability includes the ability for the FPN to send a message (e.g., email, social media, SMS/text) and no payment address alias exists in the GDS, the FPN will generate a message, referred to as an invitation, and attempt to deliver the message to the recipient. After the recipient verifies control of the account that was used to deliver the message, the FPN completes the transfer and adds a payment address alias for receipt to the GDS.

The specifics of the FPN’s technical design for interoperability with various networks are addressed below.

### U.1.6.1 Interoperability with Payment Card Networks

The FPN’s technical design is interoperable with existing payment card networks (e.g., Visa, MasterCard, Discover, American Express). The FPN achieves interoperability by allowing participants to create payment address aliases in the GDS that point to payment card information stored outside of the GDS. The FPN does not store the payment card information in the GDS; instead it creates a payment address alias to the payment information stored with the payment card network or with an approved processor of the payment card network that meets the required payment card industry standards for secure storage of payment card information. The FPN’s technical design specifies that the payment card payment address alias must only point to a payment card issued to the participant, not another party. The FPN satisfies this specification requirement by verifying the identity of the holder of the payment card before the payment card payment address alias is created in the GDS.

### U.1.6.2, Interoperability with Automated Clearing House Network

The FPN’s technical design is interoperable with the ACH network. For example, the current open source implementation of the system allows the holder to transfer value to any verified checking or savings account at a depository institution in the United States. The FPN achieves this interoperability by allowing participants to create aliases in the GDS that point to the routing number and account number of the participant’s account with a depository institution. To improve security and to comply with regulations, the FPN specifies that the payment address alias must only point to an account owned by the participant and not another party.

### U.1.6.3, Interoperable with Social Media Networks

The FPN’s technical design is interoperable with social media networks. For example, the current open source implementation of the system is interoperable with Facebook, Twitter, and LinkedIn. The FPN achieves interoperability by allowing participants to create payment address aliases in the GDS that point to the participant’s profile on a social media site. To improve security, the system specifies that the participant must verify control of the social media profile by successfully authenticating from the FPN to the social media site using OAuth2. After the participant has successfully verified control of the profile on the social media site, the FPN stores a social media site payment address alias. After the payment address alias has been added and stored in the GDS, Payers can use the social media site profile address of the Payee on the payment order to immediately transfer funds to the Payee.

### Interoperable with Email Systems

The FPN’s technical design is interoperable with email systems. For example, the current open source implementation allows an enrolled participant to add an email address payment alias for most email systems. The FPN achieves interoperability by allowing participants to add email payment address aliases in the GDS that point to the participants’ verified email addresses. The FPN specifies that the participant must verify control of the email address before the email payment address alias will be added to the GDS. After the email payment address alias has been added to the GDS, Payers can use the email address of the Payee on the payment order to immediately transfer funds to the Payee.
Interoperable with Mobile Carrier Networks’ Short Message Services

The FPN’s technical design is interoperable with mobile carrier networks’ Short Message Services (SMS). The FPN achieves interoperability by allowing participants to add a cell phone number payment address alias to the GDS that points to the participant’s verified cell phone number. The participant verifies control of the cell phone number by authenticating to the FPN, adding the participant's cell phone number, and successfully responding to a SMS message sent by the GDS. After the participant successfully verifies control of the cell phone number to the GDS, a cell phone payment address alias is added to the GDS. Then Payers can use the cell phone number of the Payee on the payment order to immediately transfer funds to the Payee.

Interoperable with Personal Contact Applications and Directories

The FPN’s technical design is interoperable with contact applications and directories like the iOS Contacts app. The FPN allows developers of personal contact applications and directories to integrate with the system using the API.

U.1.6.4, Interoperability with Point of Sale Systems

The FPN’s technical design is interoperable with Point of Sale systems like MICROS. The FPN allows the owners and/or developers of Point of Sale systems to integrate with the FPN using the API.

U.1.6.6, Interoperability with Financial and Accounting Systems

The FPN’s technical design is interoperable with Financial and Accounting systems used by Financial Institutions like FIS and Jack Henry. The FPN allows owners and/or developers of Financial and Accounting Systems to integrate with the FPN using the API.

U.2, Usability

Usability means that the Solution should provide a straightforward and simple end-user experience and be available anytime, anywhere, any way, using a variety of access points.

U.2.1, Broad Availability

The Solution should be available to end users in a variety of circumstances, and through a variety of channels, devices, and platforms (e.g., in person without a mobile device, in person with a mobile device, remote with a mobile device, online, etc.).

The FPN’s technical design provides an API that allows providers and integrators who meet the participation requirements and that have developed a published application with the ability to provide end users with access in a variety of channels and with various types of devices (e.g., desktop computers, tablets, smartphones, etc.).

The FPN supports communication via e-mail, SMS/text, and social media and notification for Integrators using the API (e.g., Google Wallet, Apple Wallet, Uber, etc.).

The technical design of the FPN supports devices that can run a supported browser and have a connection to the Internet including smartphones, tablets, personal computers and other similar devices (e.g., nook, Kindle Fire).
Payers are required to have an Internet connection with a supported browser (or published application), and enough bandwidth to authenticate, complete, sign and submit a payment order. Internet connection requirements for Payees vary depending on requirements of the Payee. The table below illustrates payment address configurations by use case that require an Internet connection to validate a payment code (i.e., preauthorized payment) before the payment can be received by the Payee.

| Payee Internet Connection Requirements by Use Case and Payment Address Configuration |
|---------------------------------|----------------|----------------|----------------|----------------|
| Payment Codes (pre-authorization) | Payee Optional | Not Applicable | Payee Optional | Not Applicable |
| Payee Internet Connection Required | Yes (if Payee has turned on Payment codes) | No | Yes (if Payee has turned on Payment codes) | No |

In the P2P use case, Payees that have previously enrolled are not required to have an Internet connection to receive a payment. Payees that have not previously enrolled, receive a payment invitation (i.e. notification) from the FPN indicating that a transfer is pending. The FPN requires the Payee to enroll before the transfer associated with a payment invitation can be completed. The FPN permits the Payer to cancel a Payment Invitation prior to the Payee’s enrollment in the FPN and acceptance of the Payment Invitation. When the Payee accepts the Payment Invitation, the FPN completes the transfer and the payment is final.

In the B2B and P2B use cases, the Payee is required to validate a payment code (i.e., pre-authorization) when the Payee’s payment address is configured “to confirm received payments”. Validation of the payment code requires the Payee to have an Internet connection.

Like payment invitations, Payers can cancel payment codes before the payment code is validated by the Payee. When the Payment Code has been validated by the Payee, the FPN completes the transfer and the payment is final.

**U.2.2. Initiating Payments with Limited Information**

The Solution should enable an entity to initiate a payment with limited information (e.g., with a name, email address, and/or phone number) as appropriate for each use case and in a way that sufficiently supports receiver authentication.

The FPN’s technical design enables an entity to initiate payments with the following methods: email, mobile phone number, social media address (Facebook, G+, Twitter, LinkedIn, etc.), by visiting a primary payment address of a Payee in the GDS with the browser, by visiting the custom payment address of a Payee in the GDS, by visiting the secure payment widget posted by a Payee on another website, and with a published application developed by an integrator.
The FPN supports transfer notifications to end users using social media sites (e.g., Google+, Facebook, Twitter, LinkedIn etc). An end user must successfully link her social media account on a supported social media site to her payment address using her social media credential before transfers sent to the social media account can be completed by the FPN. Unless the Payee has already linked a social media account to her payment address, A Payer initiating a transfer through a social media account may cancel the invitation prior to the FPN completing transfer.

View a demonstration of how a Payer sends a payment to a Payee using a Facebook profile.

The FPN also enables an entity to display an icon or vanity URL on various items to make it easier for Payers to find a Payee and initiate a payment. This principle is similar to the use of social media icons or vanity URLs (e.g., fb.com/smartmart) that are often placed on external websites or documents to invite those who view it to visit the entity’s social media site. For example, vanity URLs (e.g., fednotes.net/smartmart) can be added to business cards, advertisements, external websites, invoices, etc., to signal to payers that a payee accepts payment through the FPN. The following graphic illustrates how a vanity URL can be added to a charity organization’s business card.

U.2.3, Constant Accessibility

The Solution should be accessible to end users on a 24x7x365 basis, including to initiate the payment, have visibility into payment status, and receive final availability of good funds (see F.5, Prompt Visibility of Payment Status on page 134).

Because the FPN is an Internet service and the Payer’s signed payment orders are executed by computers without the need for human intervention, the FPN is available to end users on a 24x7x365 basis to submit payment orders, see the status of transfers, and to receive final availability of good funds in central bank money.

View the system being accessible, initiating a Payer’s payment instruction and allowing Payees to receive final availability of funds.
**U.2.4, Ease of Use**

The Solution should be easy to use, accommodate varying levels of End-User technological proficiency, and address the usability needs of individuals with disabilities, the elderly, and individuals with limited English proficiency.

The FPN is easy to use. The Payer’s payment address is the source of funds (i.e., Fed notes) for each transfer. To complete a transfer, the Payer specifies the Payee’s payment address, the amount of the transfer and clicks send to sign the payment order. The FPN then executes the payment order according to the Payer’s instructions.

A Payee’s payment addresses can be aliased to common devices like cell phone numbers, email addresses, other domain addresses controlled by the Payee, social media accounts (see U.2.2), and other types of devices.

The FPN’s technical design addresses the needs of the elderly and individuals with varying levels of end user technological proficiency, disabilities, and limited English proficiency in the following ways that meet Web Content Accessibility Guidelines (WCAG) 2.0 published by the W3C:

- Color is not used as the only way to visually communicate to end users required or optional actions.
- The FPN can be resized without the use of assistive technology without losing content or functionality or requiring end users to scroll horizontally to view content.
- The FPN does not contain background audio or audio that plays automatically and therefore does not interfere with end users who use assistive technology (e.g., screen readers).
- Most actions taken by end users do not involve a time limit. Actions that do involve a time limit (i.e., paying with payment codes) allow end users to set and modify the time limit.
- End users can reauthenticate to the FPN to complete a payment without the loss of information if the end user is not able to complete a payment in a single session.
- The FPN does not contain flashes that would affect individuals prone to seizures.
- An error message containing explanatory text is displayed to end users if an error occurs.
- The FPN uses clear and simple language to communicate to end users.
- The FPN uses readable fonts.
- The FPN uses non-text content purely as decoration.

**U.3, Predictability**

Predictability means that the Solution should have a reliable and standard end-user experience for its baseline features.

---

37 [Web Content Accessibility Guidelines (WCAG) 2.0](http://www.w3.org/WAI/WEBSAF/), published by W3C.
U.3.1, Delivery of Core Features

The Solution design should ensure that its components and supporting parties collectively deliver the defined baseline of core features.

The FPN’s technical design specifies that the Federal Reserve will control an Internet domain (e.g., fednotes.net) for the issuance and publication of Fed notes. In addition to the publication of Fed notes, the web domain will serve as an integrated GDS. All U.S. consumers and businesses including providers are free to enroll at the web domain to establish payment addresses in the GDS for the purpose of holding and transferring Fed notes. The FPN’s design also specifies that an API is available to allow providers and integrators to provide value added services. These components, operated by the Federal Reserve and the Governing Organization for the benefit of the public, constitute the baseline features of the FPN.

Click to view a demonstration of how the system allows for a web domain that is controlled and operated for the issuance and publication of Fed notes.

U.3.2, Communication of Core Features to Users

Baseline features of the payment experience (timing, legal rights, costs, risks, etc.) should be defined, documented, and communicated such that they are well known by end users and compliant with consumer protection and commercial law (see L.1 and L.3). Aspects that might vary from one payment to the next (such as fees, timing, etc.) should be communicated by the provider to the end user in advance and at the time of each payment. Communications should be appropriate for the audience, uniform, clear, concise and easily understood so that they can be incorporated into decision making.

The FPN’s user interface displays all the information an end user needs to know to understand and use the FPN including baseline features, definitions of terms, and prompts for how to perform tasks. Aspects of the FPN that may vary from one transfer to the next, such as fees and timing, are communicated by the FPN to the end user in advance of each payment. All communications are context sensitive, appropriate for the audience, uniform, clear, and concise, so they can be easily understood and incorporated into decision making. The operation of the FPN and communication with the end user are done in compliance with consumer protection and commercial laws.

Click to view a demonstration of how the baselines features are built into the end user’s payment experience.

---

38 The Federal Reserve’s issuance of Fed notes includes a process for the Federal Reserve to cryptographically sign each Fed note. A public key is available on the Internet domain to validate the signature of the Fed note.
39 Enrollment in the GDS requires individuals to establish a secure credential (see S.10).
U.3.3, Standard Messaging Protocols
To facilitate a consistent experience for end users’ interaction with each other and with other entities (e.g., providers) the Solution should use standard communication and messaging protocols.

The FPN uses Internet standard communication and messaging protocols to provide a consistent experience for end users. Internet standard communications include the use of Domain Name Services (DNS), Secure Hypertext Transport Protocol (HTTPS), Hypertext Markup Language 5 (HTML5), Uniform Resource Identifiers (URIs) or Uniform Resource Locators (URLs), Cascading Style Sheets (CSS), Portable Network Graphics image files (PNG), JavaScript, and other standards and languages (see S.7.1-Components and controls that leverage and are consistent with industry standards, S.10.3.)

U.3.4, Availability of Core Features
Baseline features should be provided consistently, regardless of the end user’s choice of channel, form factor, or providers (see E.1, Enables Competition on page 84).

The FPN’s baseline features are specifically limited (see U.3.2) so that they are provided consistently regardless of end users choice of form factor, providers, or integrators. Providers and integrators use the API to add value to the baseline features.

View a demonstration of how the baseline features are consistently provided to end users.

U.3.5, Clearly Defined Error Resolution
The error resolution protections, rights, and liabilities of the Payer and Payee should be clearly defined and easily understood by all parties as it relates to them (see S.5).

The terms and conditions of the FPN including error resolution protections, rights, and liabilities are clearly defined in published documentation (e.g., help, FAQ and participation agreements). The documentation is modified as needed by the FPN’s Governing Organization.

Because the Payer’s signed payment orders are executed by computers according to the Payer’s instructions, it is possible for the Payer to initiate an unintended payment. To help prevent Payer errors, the system is designed to assist the Payer through the payment initiation process and verify the Payer’s intent. The way to avoid unintended payment is to assist the Payer with knowledge that she is completing the payment order with the correct Payee. For example, the FPN can prompt the Payer with a message that says, “You’ve never sent to this person before. Are you sure?” The FPN cannot completely prevent unintended payments, but there is much that can be done to help avoid unintended payments, including integration with personal contacts, apps, and directories, and allowing the Payer to select from a personal contact list.

View one example of the FPN’s error resolution protections.
U.3.6, Distinctive Terminology

The Solution should be easily described by a commonly understood generic, brand-agnostic, term that clearly distinguishes it from other payment methods (e.g., like “check” or “cash”). Key goals of the common term are to increase adoption, confidence, and understanding of the Solution, thereby decreasing potential for confusion.

Several generic terms that could be used to define the FPN:

- digital banknotes
- Federal Reserve Notes (Fed notes)
- digital currency
- digital cash
- E-cash

The author suggests that the Federal Reserve, the Faster Payments Task Force and the Secure Payments Task Force determine an appropriate, commonly understood, brand-agnostic term to clearly distinguish this method from other payment methods.

U.4, Contextual Data Capability

Contextual data capability means that the Solution should support the transfer or association of relevant information needed by end users. Such information describes the reason for, or is otherwise related to the funds transfer, as appropriate to the use case.

U.4.1, Types of Contextual Data

Contextual data, depending on the use case, might include, for example, biller reconciliation information, extended remittance information, Payer and Payee names and locations (as recognized by other parties to the transaction), tax payment information, information to facilitate investigations of possible fraud or error, loyalty/rewards information, and a short message to accompany payments.

The FPN records, retains, protects, discloses, and makes available to the Payer, Payee, and Issuer as permitted by the rules appropriate contextual data. Contextual data may include but is not limited to the following:

- Transfer identification (each transfer is assigned a system-wide, unique ID)
- Transfer type (transfer types as defined by the system)
- Date and time the transfer was started
- Date and time the transfer was completed or ended
- Status of the transfer
- Amount of the transfer
- Visibility of the transfer (i.e., public or private)
- Appropriate details about each participant or stakeholder involved in the transfer
- Fed notes involved in the transfer by unique identifier and
- Closed-loop notes involved in the transfer including the type of the note (e.g., gift, loyalty, rewards, promotional), the name the notes Issuer, the denomination, and the date of issuance
Faster Payments Network Solution Proposal

The FPN may also capture and record contextual data that include channel and/or device specific information. For example, data may include device operating system, device hardware identifiers, device application identifiers, or device location information.

Contextual information associated with a transfer can be viewed by a stakeholder of the transfer to perform all types of responsibilities including but not limited to updating double entry accounting systems, preparing reports, preparing tax statements, auditing, and investigating errors.

- View how the FPN records, retains, protects, discloses and makes available to the Payer, Payee, provider(s) and Issuers appropriate contextual data.

**U.4.2, Integration of Contextual Data**

The Solution should enable easy integration of contextual data with interfacing business and personal finance systems (e.g., accounts payable, accounts receivable, claims processing, payroll, treasury workstation, Consumer accounting software, tax reporting software, etc.) where needed.

The FPN’s technical design allows simple integration with business and personal finance systems, including accounts payable, accounts receivable, claims processing, payroll, treasury workstation, and consumer accounting software. Integration is enabled through a standards based (i.e. HTTP, JSON) Application Programming Interface (API) with remote procedures and functions calls available for popular development languages, including Java, C, C++, Python, Ruby, Javascript, Perl, and PHP.

**U.4.3, Availability of Contextual Data**

The Solution’s approach to transferring or associating contextual data should balance the need for flexibility/adaptability with the need for standards.

The stakeholders for any transfer have access to contextual data through customized applications over any web browser and any current or future operating system. They can also use the API to access and retrieve contextual data in common data-interchange formats (e.g., XML, JSON etc). The API will be kept up to date so that contextual data is provided in the standard data-interchange formats.

**U.5, Cross-Border Functionality**

Cross-border functionality means that the Solution should enable convenient, cost-effective, timely, secure and legal payments to and from other countries.

**U.5.1, Convenient, Cost-Effective, Timely**

The Solution should provide a convenient, cost-effective and timely cross-border payment method. Any special cross-border considerations for additional security measures (beyond those covered in S.1-S.11) should be addressed.

The FPN’s technical design enables convenient, cost-effective and timely cross-border payments.
Faster Payments Network Solution Proposal

The FPN is convenient because it can be accessed anytime using an Internet-connected device running a supported application (such as a web browser or mobile app). Payees are notified of received payments through their preferred communication channels.

The FPN is cost-effective because the transfer of value may be denominated in any supported currency held by the Payer, including closed-loop currency (i.e., Brand Cash), and the transfer has no transfer cost associated with it. The amount sent by the Payer is the amount received by the Payee.

The FPN is timely because all transfers are completed immediately. Because the FPN is an Internet service, transfers can span geographical borders and time zones. For example, a U.S. consumer enrolled in the FPN and traveling in Mexico can receive an immediate transfer in Fed notes at any time during the day or night.

View how the FPN is a convenient, cost-effective, and timely cross-border payment method.

U.5.2, Interoperability with Similar Payment Systems

The Solution should allow for interoperability with similar payment systems in other countries (see E.4 for an example of how interoperability may be facilitated). Relevant interoperability considerations might include differences in messaging standards, languages, character sets, mandatory data elements, party/account identifiers, regulatory considerations, and timing of settlement and good funds availability.

Because the FPN’s technical design supports multiple issuers and currencies, any Central Bank, operating under a participation agreement, can issue its national currency as part of the GDS. The optimal implementation of the FPN would use a single, distributed GDS; however, it is possible for a Central Bank in another country to establish and operate its own GDS.

The FPN is also compatible with dissimilar networks including the ACH network, the payment card networks, and other networks (e.g., Dwolla, Ripple, FAST)

View an example of the FPN allowing an approved Central Bank to issue their currency into the GDS.

U.5.3, Advance Disclosure by Providers

The Solution should require providers to make advance disclosure (both prior to and at the time of the Payer initiating the payment) of fees, exchange rates, and other end-user costs, as well as the timing of good funds availability and any risks with the payment, consistent with regulatory requirements.

The FPN’s technical design satisfies this consideration statement by:

- Ensuring that participants agree to the terms and conditions of the FPN, including the fees and risks for certain types of transfers
Faster Payments Network Solution Proposal

- Allowing Payers to send money to a Payee freely, without transfer fees
- Disclosing exchange rates to the purchaser when exchanging notes denominated in one national currency for notes denominated in another national currency
- Displaying fees that are required of the Payer for certain types of transfers (e.g., deposit to checking account)

The transfer between payment addresses is executed in the national currency as specified by the Payer when the signed payment order is submitted. The Payee receives the payment as initiated by the Payer without requiring currency conversion. The Payer may elect to purchase a different national currency prior to the transfer to the Payee. Alternatively, the Payee may purchase a different national currency after receipt of the payment from the Payer. Exchange rates, conversion costs and/or fees are disclosed to the purchaser (i.e. Payer or Payee) of a national currency at the time of purchase. The process of transferring national currency is separate from the process of exchanging national currency, and transfer doesn’t require conversion.

U.5.4, Currency Conversion

The Solution should allow conversion from one currency to another as necessary for cross-border payments.

The FPN’s technical design allows for conversion from one currency to another as necessary for cross-border payments by: 1) separating the conversion process from the transfer process for cross-border payments, 2) allowing the Payer to determine the currency to transfer to the Payee, 3) allowing the Payee to receive the currency sent by the Payer, and 4) allowing the Payee to convert the currency as desired and with any number of conversion exchange providers offering the currency exchange services.

U.5.5, Cross-Border Payments

If the Solution does not have cross-border functionality at implementation, it should have a credible plan for implementing cross-border payments in the future. The plan should demonstrate credibility by showing the timeline for cross-border implementation and how the other considerations of this criterion will be addressed.

The proposed implementation of the FPN will support all national currencies at implementation. The number of currencies available for cross-border transfer at implementation is dependent on the participation of financial institutions that issue other national currencies.

U.6, Applicability to Multiple Use Cases

Risk applicability to multiple use cases means that the Solution should support payments in multiple use cases (including at least one targeted use case), and should demonstrate its ability to be extensible and flexible to additional payment use cases in the future.

The FPN’s technical design enables payments for all the targeted use cases in addition to many future use cases.

The FPN allows individuals and all other entities to hold and transfer Fed notes for payment. Because the Fed notes use standard denominations (i.e., $.01 to $100), they are ideal for either low-value or high-value payments. Additionally, a Payer can send a payment to another person or entity either in person or remotely. All transfers using the FPN are immediate and final.
The following table illustrates the use cases that are supported by the FPN at implementation irrespective of the value of the payment and provides examples of supported types of payments.

<table>
<thead>
<tr>
<th>Example Payment Types by Use Case at Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government</strong></td>
</tr>
<tr>
<td>Funding of programs, and intra-departmental payments</td>
</tr>
<tr>
<td>Taxes, fees for licenses and permits, fines</td>
</tr>
<tr>
<td>Taxes, utilities, fines, and fees</td>
</tr>
</tbody>
</table>

The examples listed reflect the FPN’s ability to support multiple devices, including printers, fax machines, vending machines, kiosks, and airport cart rental systems. The examples also show the FPN’s applicability to multiple end users, such as a student paying for a copy at a university copy center, a mother renting a cart to carry luggage at the airport, and an employee purchasing a drink from a vending machine. The examples listed above are not the only types of payments supported.

The FPN’s technical design also supports the following targeted uses cases:

- B2B - ad hoc low-value, remote, real-time
- B2P - ad hoc high-value, remote, real-time
- B2P - ad hoc low-value, remote, real-time
- P2P - in-person and remote, real-time
- P2B - ad hoc in-person and remote, real-time

View how the FPN performs payments for each of the following use cases:

- B2B - ad hoc low-value, remote, real-time
- B2P - ad hoc high-value, remote, real-time
- B2P - ad hoc low-value, remote, real-time
- P2P - in-person and remote, real-time
- P2B - ad hoc in-person and remote, real-time
Part C, Section 2: Efficiency

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VE</td>
<td>E</td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.1, Enables Competition</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.2, Capability to Enable Value-Added Services</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.3, Implementation Timeline</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.4, Payment Format Standards</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.5, Comprehensiveness</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.6, Scalability</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E.7, Exceptions and Investigations Process</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

E.1, Enables Competition

Enables competition means the Solution should allow providers to compete with each other to offer services.

E.1.1, Choice of Providers

The Solution should allow choice of providers based on factors including, but not limited to, services and price.

The FPN’s technical design allows providers, integrators, developers and third parties to compete with each other on a variety of factors including price, services provided, channel access, device access, integration, user experience, and value-added features. Competition is achieved when integrators develop value-added features and services that extend the baseline features using the GDS and the API. See Figure 1: Interoperability with Payment Card Networks on page 50 for a visual example of integration.

E.1.2, Switching Providers

The Solution should allow any entity to easily switch among providers and/or use multiple providers.

The FPN is Internet-based, so value held by an entity can be represented in multiple integrator applications at the same time but spent by the entity only once. Each integrator’s application can customize its user experience, allowing integrators to differentiate themselves through branding, user experience, and value-added services. The ability to switch between integrators is as simple as opening another application developed by an integrator.
For example, an end user may use an integrator’s application developed by a fast food chain (e.g., McDonalds, Wendy’s, Burger King, Carl’s Jr., etc.). Because the restaurant chain hired an integrator to develop the mobile application, the value held by the end user is displayed in the application when opened on the end user’s mobile device. The end user can open a different mobile application, from a different restaurant chain, developed by a different integrator and see the value he holds displayed there as well. The value displayed in any mobile application is updated in real time to reflect transfers made by the end user.

E.1.3, Disclosure to Customers

The Solution should require a given provider to disclose in advance to their customer, information necessary to easily understand the total cost of using that provider.

The following examples illustrate the FPN’s capability for an integrator to disclose to the customer the costs associated with using any provider:

- Joel exchanging a foreign currency with a depository institution.
- Adrian’s Cafe paying a deposit fee for an automatic daily deposit through the ACH network (costs less because of the small delay associated with ACH).
- Smartmart paying a deposit fee for an automatic, direct, and immediate deposit (costs more because the deposit is direct and immediate).
Joel Exchanging Foreign Currency with a Depository Institution

The following example illustrates how a provider of currency exchange services is required to disclose in advance to a customer the total cost of using that provider for currency exchange.

Joel is holding $250 USD in Fed notes and desires to exchange $100 USD for Mexican Pesos (“MXN”) issued by Banco de México. Joel finds an exchange provider offering $18.00 MXN for every exchanged $1 USD, plus a one-time fee of $5.95. Joel finds a second currency exchange provider that offers $17.70 MXN for every exchanged $1 USD, plus a $3.95 one-time exchange fee. Both currency exchange providers disclose to Joel the total cost of the exchange by showing him the MXN he will receive for the amount he is sending, illustrated in the table below as follows:

<table>
<thead>
<tr>
<th>Bank Uno Currency Exchange Service</th>
<th>Bank Dos Currency Exchange Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convert From:</td>
<td>Convert From:</td>
</tr>
<tr>
<td>$100 USD</td>
<td>$100 USD</td>
</tr>
<tr>
<td>Convert To:</td>
<td>Convert To:</td>
</tr>
<tr>
<td>$1800.00 MXN</td>
<td>$1770.00 MXN</td>
</tr>
<tr>
<td>Fees:</td>
<td>Fees:</td>
</tr>
<tr>
<td>$5.95 USD</td>
<td>$3.95 USD</td>
</tr>
<tr>
<td>Total you pay:</td>
<td>Total you pay:</td>
</tr>
<tr>
<td>$105.95 USD</td>
<td>$103.95 USD</td>
</tr>
<tr>
<td>Total you receive</td>
<td>Total you receive</td>
</tr>
<tr>
<td>$1800.00 MXN</td>
<td>$1770.00 MXN</td>
</tr>
<tr>
<td>Exchange Rate: $1 USD = $1800.00 MXN</td>
<td>Exchange Rate: $1 USD = $1770.0 MXN</td>
</tr>
</tbody>
</table>

Joel determines that the second provider is the best value for him, so he makes the exchange with the second currency exchange provider.

The FPN’s technical design to support such a required disclosure is a payment order dialog from the provider (see example currency conversion payment order dialog below) that allows Joel to enter the amount he wants to send in USD and shows the amount he will receive in MXN. When Joel has made the decision to execute the exchange, he can do so with the click of a button. One important aspect of this exchange is that the MXN is returned to Joel. He is then allowed to transfer MXN to family and relatives. He knows exactly how much each recipient will receive in MXN because the payment system allows Joel to hold and transfer MXN.
Adrian’s Cafe paying a deposit fee for an automatic daily sweep through ACH

The following example illustrates how a depository institution that accepts Fed notes for deposit discloses in advance to the customer the total cost of making the deposit.

Mark owns Adrian’s Cafe. His business receives payment from his customers in Fed notes. Mark’s depository institution allows him to deposit digital Fed notes into the Adrian’s Cafe business account. Each deposit costs Adrian’s Cafe $.25. To save transfer costs, Mark has turned on automatic sweep for the Adrian’s Cafe business wallet so that funds are deposited once each business day at 4:30 p.m.

The FPN required the depository institution to display to Mark the cost of each deposit when he turned on the automatic deposit feature.

Smartmart paying a deposit fee for an automatic, direct and immediate deposit without ACH

The following example illustrates how a depository institution that accepts Fed notes for deposit discloses in advance to the customer the total cost of making a deposit.

Jeff is a treasurer for Smartmart, a large retailer. Smartmart receives a significant portion of its payments in digital Fed notes. Jeff has opened an account for Smartmart that will allow Smartmart to make immediate deposits to its commercial checking account for all of its locations. Although Jeff has agreed to pay a fee of 30 basis points per $100 deposited, the cost represents a savings to Smartmart over their current deposit process that takes one day to process. Jeff turns on auto sweep for every Smartmart location. Now for every $100 in digital
Fed notes received in a Smartmart wallet, the funds are automatically and immediately deposited into the Smartmart commercial checking account.

The FPN required the depository institution to display to Jeff the cost of each deposit when he turned on the automatic deposit feature.

View a demonstration of a business paying a fee to make a deposit to an account with a depository financial institution.

**E.1.4, Providers Allowed to Provide Services**

The Solution should allow providers, regardless of their size or incumbency, to provide services as long as the providers meet participation requirements (see S.11).

Integrators that meet the participation requirements are able to use the API to provide baseline features, value-added services, and differentiated user experiences in their applications for their customers. Because integrators do not have to establish accounts with balances for end users when developing applications that use the FPN, special requirements (e.g., capital requirements, bonding, etc.) need not be a participation requirement for an integrator. Furthermore, the FPN’s technical design makes it possible for an integrator to freely develop an application but gives control and publication of the application to the Governing Organization; thus, it is possible for integrators of all sizes to develop applications that provide the baseline features, value-added services and unique customer experiences.

**E.2, Capability to Enable Value-Added Services**

Capability to enable value-added services means that the Solution should enable providers to offer additional services beyond the Solution’s defined baseline features.

**E.2.1, Provider Integration**

The Solution should allow providers to integrate with the Solution using open and accessible standards to offer value-added services to any entity.

The FPN enables integrators to offer additional services beyond the FPN’s defined baseline features by:

- Allowing businesses to use the GDS to issue closed-loop value.
- Allowing integrators to enhance the baseline features through the use of an open HTTPS API.

Near future improvements planned for the FPN include additional development language modules for popular programming languages including C, C++, java, python, perl, ruby, php, etc. These modules will spur a wave of safe payment innovation that will allow integrators to rapidly deploy value-added services for many entities, accelerating adoption and achieving FPN ubiquity.
View an example of how providers can use open and accessible standards, including open development languages, to enhance the baseline features.

**E.2.2, Value-Added Features**

The Solution should allow providers, regardless of their size or incumbency, to provide value-added features as long as the providers meet participation requirements (see S.11).

Depository institutions of all sizes and incumbency provide the service of distributing the Fed notes to their customers. All providers meeting the participation requirements can be integrators and develop custom or enhanced interfaces, software applications, mobile applications, and web services, which are considered value-added features.

The participation requirements for integrators to develop value-added features do not need to include capital requirements, establishing an anti-money laundering program, or bank secrecy act reporting because notes are issued by the Federal Reserve, distributed through depository institutions that have an account with the Federal Reserve, and AML and BSA reporting are handled for all integrators at the governance level. Consequently, integrators of all sizes that meet the participation requirements will be able to participate. Also see response in **E.1.4, Providers Allowed to Provide Services** on page 88.

Integrators have an opportunity to develop value-added features and custom end user experiences. Integrators must demonstrate a proficiency in development using the API, which will be verified through a rigorous testing and certification process before the applications can be made available to end users.

**E.2.3, Disclosure Required**

The Solution should require providers to clearly disclose to their customer that value-added services are optional.

Integrators offering value-added services through the API are required to request permission from the end user to access certain baseline features. At the time such permission is requested, the FPN will disclose to the end user, using appropriate legal language, that all other features offered through the integrator’s application are optional and not part of the baseline features and, therefore, are provided by the integrator to the end user under separate terms and conditions. The FPN will also ask the end user to check a box next to the disclosure language to confirm that the end user has read the disclosure before permission to the integrator’s application is granted.

Integrators may also provide other value-added services, and the FPN will communicate that such services are optional. For example, optional services like closed-loop cash offers may be made available to end users. Closed-loop offers are configurable and require the creator of the offer to disclose all relevant information about the offer, including the amount of the offer, the payment types accepted, limitations on redemption (including expiration or a cap on the amount of that can be held in the wallet), and the allowed maximum number of offer purchases.
View how a provider makes closed-loop value available to customers.

**E.3, Implementation Timeline**

Implementation timeline means that the Solution should have a credible plan to achieve initial implementation and ubiquity (as defined in the glossary) by the target dates described in the effectiveness scale below.

**E.3.1, Credible Plan for Implementation**

The Solution should demonstrate a credible plan by explaining how implementation will be funded, what implementation and ubiquity hurdles might arise, what plans exist to overcome the hurdles, which entities expect to adopt the Solution, what market share and growth projections are used, and how the projected timelines compare to similar historical examples. The credible plan should support comprehensiveness as defined in E.5.

**E.3.1.1, Credible Plan to Achieve Implementation by 2018 and Ubiquity by 2020**

The credible plan to achieve implementation by 2018 includes the table in Part B: Business Considerations on page 49. The implementation timeline table in the Business Considerations section shows high-level tasks that need to be completed to implement the FPN by 2018. The objective of the implementation plan is to launch the service mid-2018 with excess resources and capacity that allow it to achieve ubiquity by 2020. The proposal suggests that the path to ubiquity is to ensure the following:

- Adoption and use by federal, state and local governments for government-to-person and person-to-government payments
- Adoption and use by the top 50 retailers (e.g., Walmart, Target, Costco, Kroger, Home Depot, Amazon, etc.) to enable consumers and businesses to purchase goods and services using the FPN
- Integration with the top point-of-sale developers to enable FPN compatibility with POS systems
- Integration with the top mobile wallets and payment apps (e.g., Apple Wallet, Google Wallet, Samsung Pay)
- Commitments from the top 50 retailers to offer rewards and/or loyalty to consumers for paying with Fed notes
- Distribution and deposit of Fed notes with top consumer and business depository institutions

**E.3.1.2, Funding for the Implementation of the FPN**

Implementation and ongoing data center operation will be funded by the Federal Reserve, who can expect to achieve full recovery of investment costs over the long run by reducing or eliminating the following costs related to providing physical currency: printing costs, transportation costs, and destruction costs. The FPN also allows the Federal Reserve to continue to recognize seigniorage for Fed notes placed in circulation. The FPN proposal recommends funding by the Federal Reserve so that the baseline features of the FPN will be freely available to every U.S. consumer and business and to ensure that the interests of consumers and businesses
have a higher priority than commercial interests. Additionally, the Federal Reserve oversight, control and funding will ensure that the additional objectives of ubiquity, safety, and efficiency are appropriately realized and balanced among competing interests. The inclusion of the FPN (e.g., digital FedCash and GDS) as a part of the Federal Reserve's products and services will allow equitable participation by all depository institutions without the Federal Reserve competing with them.

The Governing Organization will be funded by membership fees, enabling enhanced features beyond the baseline services for businesses (e.g., issuance of brand cash), performing certification of integrator applications and providing training and education services to its members and the community.

E.3.1.3, FPN Possible Implementation Hurdles

Dealing with implementation hurdles is an important aspect of every successful information technology project, especially projects of significant scale like this one. Many implementation hurdles are unforeseeable, and it is difficult to predict what implementation hurdles will arise even with small information technology projects. However, an effort to identify and understand project hurdles ahead of time improves planning and offers contingencies when hurdles arise. Many projects share common hurdles, including recruiting, hiring and retaining technical talent, the loss of key people at critical project steps, managing scope creep and change control throughout the project, aligning deliverables across multiple vendors, and clear communication of project dependencies and deadlines.

Recruiting, Hiring and Retaining Technical Talent

The competition among employers to hire technical talent is intense. Recruiting, hiring and retaining technical talent is an ongoing effort. The location and quality of offices is an important element of hiring and retaining talent. In addition to competitive compensation plans, the ability for the hiring manager to communicate a clear vision and mission for the project is critical to hiring the ideal candidate. The work to begin recruiting the executive team for the Governing Organization and implementation team should begin in early 2017 with assistance of carefully selected professional recruiters.

Loss of Key People

The loss of key people can happen in many ways (e.g., unexpected illness, resignation, death) and is not preventable. Important considerations to help address the loss of key people include complete documentation for important tasks, cross-training, and the use of written agreements for key people.

40 Organizations that join that are not grandfathered in because of their participation in the Faster and Secure Payments Task Forces.
Managing Scope Creep and Change Control

Scope creep will happen on projects both large and small—it is to be expected. Establishing a formal process to manage and approve changes will be key to managing scope creep. Another important aspect of managing scope creep is to have a clear vision of the project and a detailed plan for all work requirements, tasks and deliverables. Skilled project managers drive the project, understand the priorities and critical path, and leave room for error in the timeline. The implementation of the FPN is a significant undertaking and will take a coordinated effort from all stakeholders.

Aligning Deliverables Across Multiple Vendors and Clear Communication of Project Dependencies

The implementation of the FPN will present significant coordination and communication challenges between the Governing Organization, the Federal Reserve, the Implementation Team, and vendors that are providing products and services to the project. While some missteps with coordination and communication are inevitable, they can be mitigated with planning, the use of appropriate tools to communicate and coordinate plans, and follow-up.

The implementation team, working with the Governing Organization and Federal Reserve, are responsible for dealing with hurdles that arise and to see that milestones are achieved on time and within budget.

E.3.1.4, FPN Possible Ubiquity Hurdles

Inaccurate Scale and Capacity Projections to Achieve Ubiquity

A significant question surrounding achieving ubiquity is the question of scale and capacity planning. The current implementation has been used in local markets since 2011. Estimates for capacity planning can be made using information from experiences in the local markets. Of course estimates for capacity can and will be made for launch; however, actual usage patterns may differ from estimates. Capacity planning estimates may need to be revised quickly based on actual usage at launch and may need to be adjusted for future growth.

Priority and Integration Delays by Top Retailers

Business enrollment, integration into the point of sale, and offering consumers loyalty and rewards for using the FPN are the keys to reaching ubiquity by 2020. Businesses of all sizes have limited budgets and resources. Businesses will need time to adjust development priorities and allocate budget for integration at the point of sale. Marketing departments will also need to be provided with examples of how to use the FPN’s loyalty and rewards features to motivate consumers to adopt and use the FPN.

Adoption Delays by Federal, State and Local Governments

Federal, state and local governments, like businesses, require time to adjust priorities and allocate budgets. Adoption of the service by federal, state, and local governments is a key component of the plan to achieve ubiquity. Outreach and education will need to begin immediately to allow time for governments to act and have an impact on ubiquity by 2020.

Government

The following federal government agencies are expected to adopt and use the FPN: the Federal Reserve, the Internal Revenue Service, the Department of the Treasury, the Social Security
Faster Payments Network Solution Proposal

Administration, and the United States Postal Service. Adoption by Federal agencies will also help to drive business adoption and integration at the point of sale. Adoption by the USPS will also help drive financial inclusion by offering exchange services of physical Fed notes for digital ones in geographical areas where people do not have access to retail banking services or for people who choose to operate outside the traditional banking system.41

Businesses

The following retailers and oil and gas companies are expected to adopt and use the FPN: Walmart, Target, Costco, K-Mart, 7-Eleven, CVS Pharmacy, Rite Aid, Conoco, Exxon, Shell, Mobil, Murphy USA, and the other top-50 retailers. The top 50 retailers account for 48 percent of retail sales. Retailers will help drive consumer adoption by offering rewards and loyalty when consumers pay using the FPN. The costs of rewards and loyalty programs born by retailers will be offset by the savings realized when consumers use the FPN in lieu of a payment card for purchases. Retailers save in the following ways when a consumer chooses to pay with the FPN: savings from payment card interchange, savings from having to maintain and upgrade separate dedicated equipment (e.g., EMV terminal) other than the register or POS, savings from having to maintain PCI compliance and protecting consumer information, and savings from chargebacks.

Providers

Depository institutions and regulated non-bank providers have an opportunity to participate in the FPN at various levels. The simplest level requires no integration. Because the FPN uses Fed notes for payment and Fed notes are distributed equally by small, medium and large financial institutions, a significant percentage of depository institutions are expected to adopt and offer Fed notes to their customers.

E.3.1.5, FPN Market Share and Growth Projections

To achieve ubiquity by 2020, the FPN will utilize a top-down approach and focus on enrolling the top 50 retailers responsible for 48 percent of retail sales. The top-down approach includes obtaining commitments from government agencies to switch payments from higher cost prepaid programs to the use of Fed notes on the FPN. Because of the simplicity of enrollment, ease of use, compelling business model (i.e., free transfers, free enrollment, loyalty, rewards), and API integration capabilities, the FPN can achieve ubiquity by 2020.

E.3.1.6, FPN Projected Timeline Compared to Historical Examples

The most recent examples of growth for commercial payments products and companies include PayPal, Square Stripe, Venmo, Braintree, Apple Pay, Google Wallet, and Samsung Pay.

PayPal, founded in 1998, touts 179 million active customer accounts and 4.9 billion payment transactions on a payment volume of $282 billion for 2015.42 Visa (formerly National

42 PayPal website
BankAmericard) reported $1.2 trillion in transaction volume for the year ending March 31, 2015.\(^{43}\)

The timeline below shows it took approximately 12 years,\(^{44}\) from 1958 to 1970, for revolving, general purpose credit cards (i.e., BankAmericard) to reach 100 million cards issued—an average issuance of nearly 8.4 million cards per year. Over the next 30 years, Visa card issuance grew to reach one billion cards issued—an average issuance of 30 million cards per year, almost 3500 cards issued for every hour of every day.

<table>
<thead>
<tr>
<th>Year</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>1958</td>
<td>Bank of America introduces a general-use credit card, the BankAmericard.</td>
</tr>
<tr>
<td>1960 (Dec)</td>
<td>Almost 1 million BankAmericards card issued, with nearly 30,000 merchants.</td>
</tr>
<tr>
<td>1966 (Jun)</td>
<td>1,765,000 BankAmericards issued and 61,000 merchants.</td>
</tr>
<tr>
<td>1970</td>
<td>100 million credit cards issued. The issuers’ formed National BankAmericard Incorporated.</td>
</tr>
<tr>
<td>1976</td>
<td>National BankAmericard card renamed to Visa.</td>
</tr>
<tr>
<td>2000</td>
<td>1 billionth card issued by Visa.(^{45})</td>
</tr>
</tbody>
</table>

The timeline illustrates that to launch a payment service and to achieve ubiquity by 2020 is unparalleled in recent history. The scope of the solution includes the launch of a Faster Payments Network operated by the Federal Reserve and a Governing Organization that will provide equitable access to a system that is freely available to all U.S. consumers and businesses. The system uses digital Fed notes as the method of payment with no transfer fees. There are loyalty and rewards for users. Digital Fed notes will be initially distributed by the nation's top depository institutions, accepted for payment by the nation’s top 50 retailers, integrated into the top point of sales systems and mobile wallet applications, and can be deposited to all accounts at U.S. depository institutions by ACH.

At launch, the FPN will meet the definition of ubiquity for the person-to-person use case because any person (i.e., Payer) will have the ability to reach any other person and to deposit funds at any depository institution by ACH. The key to the FPN achieving ubiquity is business enrollment, which will enable person-to-business and business-to-business use cases. One hundred percent acceptance is not expected because no payment method, not even physical cash, is accepted everywhere. The goal for ubiquity is to enable the FPN to be accepted by the majority of businesses. Understanding precisely how the FPN achieves ubiquity is crucial to reaching the goal in a short period of time.

Three steps are required to achieve ubiquity among businesses. The first is to enroll the top 50 retailers (e.g., Walmart, Target, Costco, Kroger, Home Depot, Amazon, etc.) to accept the FPN, so any person can use the FPN to purchase goods or services from the top 50 retailers.\(^{46}\) By

---

\(^{44}\) Bank of America website.
\(^{45}\) Visa.com website.
\(^{46}\) National Retail Federation website.
engaging these businesses alone, the FPN will be accepted for 48 percent of retail sales.\(^{47}\) Second, to expand acceptance to smaller retailers, it is important for the FPN to partner with point-of-sale system developers to build compatibility with the FPN into the POS systems. If the FPN is integrated with POS systems, any retailer who uses those POS systems will be enabled to use the FPN also. Finally, it is important for the FPN to integrate with mobile wallet systems, so consumers who rely on those systems and enjoy the convenience of mobile wallets will have access to the FPN.

### E.4. Payment Format Standards

Payment format standards means that the Solution should be interoperable with current payment format standards (e.g., ISO 20022) and adaptable to future needs and standards.

#### E.4.1. Interoperation with Existing Standards

The Solution can interface or interoperate with existing payment format standards that are relevant to use cases targeted by the Solution (see U.4).

While the FPN’s technical design supports many use cases (see U.6, Applicability to Multiple Use Cases on page 82), the FPN is targeting the following use cases at implementation:

- P2P
- P2B
- B2P – ad hoc low-value
- B2P – ad hoc high-value
- B2B – ad hoc low-value

The FPN’s default message format for all targeted use cases is Javascript Object Notation (JSON). JSON is a data interchange standard of the Internet Engineering Task Force (IETF). The FPN’s technical design provides data translation to ISO and other standard message formats as needed (e.g., ISO 20022, ISO 8583).

#### E.4.2 Enables Cross-Border Interoperability (see U.5).

The Solution should enable cross-border interoperability.

The FPN’s technical design enables cross-border interoperability as follows:

- International ACH using the NACHA format
- Access to the GDS using the API in JSON format for published applications
- Data transformations to ISO and other standard message formats (e.g., ISO 20022)
- Direct end user access using supported devices and web browsers over the Internet (e.g., HTML5 format)

---

\(^{47}\) Bureau of Economic Analysis website.
E.4.3, Cost-Effective

The Solution should be cost effective to adopt.

The FPN’s technical design provides various message format options allowing integrators and providers a choice when selecting a message format. Because integrators have a choice of message formats, they can consider a range of factors when choosing a message format including cost-effectiveness to adopt, ease of integration, speed of integration, design of existing systems, etc.

E.4.4, Innovation and Updates

The Solution should facilitate innovation and be adaptable for the future by permitting a mechanism for updates.

The FPN’s technical design is innovative and provides mechanisms for future update by allowing for any number of standard message formats to be support through data transformations to/from JSON. The FPN’s utilization of this mechanism provides flexibility and adaptability to future needs and demands allowing the FPN to change in parallel with evolving and improving standards.

E.4.5, Transparency and Recognized Standards

The Solution should be transparent and developed and/or published by a recognized standards development organization.

The FPN’s technical design utilizes message formats that are transparent, developed and/or published by standards development organizations. For example, to provide access to supported devices and web browsers, the FPN uses HTML5 document markup language that was last updated and published on 28 October 2014 by the W3C. This represents the fifth revision of the HTML standard since the inception of the World Wide Web. The specification for HTML5 is freely published and available at https://www.w3.org/TR/html5/. The FPN’s technical design also supports NACHA for International ACH, JSON for the API, and data transformations to other standard message formats.

E.5, Comprehensiveness

Comprehensiveness means that the Solution should support all steps of the payment process from Initiation to reconciliation.

E.5.1, Enabling Payment Process

The Solution should enable all relevant aspects of the end-to-end payment process, including (but possibly not limited to) – initiation, payer authentication, approval by the Payer’s provider, clearing, receipt, settlement, and reconciliation. To achieve this, the Solution might build new and/or interface/interoperate with existing systems.

The FPNs technical design supports the following steps of the end-to-end payment process:

1. Payer Authentication – The Payer authenticates to the FPN.
2. Payment Order – The Payer fills in the information required for a payment order (minimally the Payee’s payment address and amount to transfer). The Payer visually verifies the
information provided on the payment order, responds to a dialog indicating that the payment order should be signed and submitted to the FPN, and the FPN executes the payment order as instructed by the Payer.

3. Receipt – The FPN updates the possession attribute to reflect the Payee as the holder of the Fed notes.

The following steps are associated with the end-to-end payment process but are either combined into the steps above or not necessary for the FPN as follows:

- Payer authorization is a part of step 2 above: Payment Order.
- Approval by the Payer's provider, applicable when a Payer is a provider.
- Clearing is part of step 3 above: Receipt.
- Settlement is part of step 3 above: Receipt.
- Reconciliation is external to the actual payment process above. Reconciliation can be either manual or automated. Manual reconciliation can be done by hand (e.g., paper ledger) or using one of many personal or business financial management software programs. The API and data streams make it possible for the approved developers of personal or financial management software to interface with the FPN for automation of the reconciliation process.

E.5.2, Support for Features

The technical design of the Solution should adequately support all of its features including its usability, reliability, performance, information security protocols, operations, compliance controls, and risk controls.

The technical design of the FPN is based on time-tested, scalable and proven Internet standards, methodologies, and technologies that support the following:

- Usability – See the following related section: U.1, U.2, U.5, U.6, E.4, S.10, F.1, F.3, and F.5,
- Reliability, See the following related sections: U.3, E.6, S.8, S.9, S.10, F.3, L.1, L.2, L.3, L.4, and G.1-2,
- Performance – See the following related sections: U.1, U.2, U.4, E.1, E.5, S.5, S.8, F.3, F.5, L.4, and G.1,
- Information security protocols – See the following related sections: U.4, E.4, E.5, S.2, S.6, S.7, S.8, S.9, S.10, L.2, L.4,
- Compliance controls – See the following related sections: E.7, S.1, S.3, S.5, S.6, S.7, S.9, S.11, F.3, F.5, L.1-4, and G.1-2,
- Risk controls – See the following related sections: U.4, E.6, S.1-11, L.1-4, and G.1-2.

E.6, Scalability

Scalability means the technical design of the Solution should readily support projected transaction volumes, values, and use cases. Adaptability means the technical design of the Solution should be able to readily adjust to ongoing environmental developments.
E.6.1, Support for Projected Use Cases

The Solution’s technical design should support projected use cases (as determined by the solution proposer) initially and over time.

The FPN’s technical design initially supports all targeted use cases (see U.6, Applicability to Multiple Use Cases on page 82) and additional use cases without modification. For example, additional use cases could include a central bank of another country issuing its national currency and utilizing the GDS for its consumers and businesses, currency exchange, and a business’s issuance of closed-loop currency and offers. The FPN uses Internet standards and is adaptable to other uses cases over time.

E.6.2, Capacity for Projected Volume and Values

The technical design should demonstrate the capacity to handle projected volumes and values (as determined by the Solution proposer), including increased transaction volumes and values during peak times or periods of stress and to accommodate a cushion above projections.

The FPN’s technical design anticipated the need for a very large number of concurrent transfers and end users, so it is designed with an internally distributed architecture that spreads the storage and query load among a variable number of databases. The FPN’s design utilizes a message-passing architecture and a workflow engine that precisely coordinates the interactions between users, databases, and automated processes. Other scalability features include internal query result caching and thorough use of short-lived database transactions.

E.6.3, Adaptable to Development

The technical design should be readily adaptable to ongoing developments, including those that are technological, economic (e.g., financial system failures, economic crises), regulatory, and customer demand driven.

Technical and Customer Demand-Driven Developments

The FPN’s technical design is readily adaptable to ongoing technical and customer demand driven developments for the following reasons:

- The technical design is based on Internet and open standards (e.g. URLs, IP, Domains, DNS, HTML5) that have been proven, regularly improved by standards organizations and adapted over long periods of time, and
- The technical design provides an open API that allows integrators to develop value-added, cross-platform services that are required to satisfy ongoing customer demands for integration into existing and new devices (e.g., smartphones, tablets, desktops, vending machines, printers), and user applications with updated or new user interfaces that are driven by ongoing updates to operating systems (e.g., Windows, iOS, OSx, Android, Chrome OS, Linux).

Economic and Regulatory Developments

The FPN’s technical design is readily adaptable to ongoing economic and regulatory developments for the following reasons: 1) the physical locations for the network operating centers and data centers can be distributed and in various geographic locations to provide required redundancy and duplication to mitigate for failures and crises, 2) equally important, the
services are uniquely offered by the Federal Reserve and the Governing Organization and offered through a single, universally trusted, and authoritative Internet domain controlled by the Federal Reserve to provide the economic stability that only the Federal Reserve can provide.

**E.7, Exceptions and Investigations Process**

Exceptions and investigations process means that the Solution should provide end users, providers, and any other relevant Parties with tools and protocols to minimize, identify, investigate and resolve exceptions.

**E.7.1, Tools to Repair Exceptions**

The Solution should provide tools, including messages, alerts, notifications and related protocols, as appropriate to end users, providers, and any other relevant parties, to support the ability to work together to repair or otherwise address exceptions in a reasonable time frame that is, at a minimum, compliant with applicable law and regulations (see S.5 and L.1).

The FPN’s architecture and tools are designed for central messaging, notifications, monitoring, administration and management of all processes and events that operate on the FPN. These processes and events can be centrally viewed, reviewed and managed at a central platform operations center to maintain service level commitments and expectations of the providers and end users. The centralization of the tools for monitoring and maintaining the operation of the platform reduces management complexity, cost, and training requirements and streamlines the operation of the FPN.

**E.7.2, Information Retention**

The Solution should ensure that information is created, recorded, and retained for an appropriate period of time to facilitate post-transaction evaluation. For example, the Solution may facilitate case management tools with the ability to trace previously originated payments and track incidents and exceptions.

The FPN’s technical design allows for it to capture, record, and retain information for an appropriate period of time, as specified by operating rules, information retention policy, law and/or regulation, and to facilitate post-transaction evaluation. The FPN captures and stores information relevant to every transfer, including payer information, payee information, and transfer information including the Fed notes involved in the transfer, transfer type, transfer status, transfer start and end date, transfer start and end time, amount, IP address, and geolocation information. If the transfer is conducted through a published application, then the FPN will also capture additional information, including information about the application, the developer of the application or integrator, and the application’s permissions at the time of transfer.

**E.7.3, Aggregate Exceptions**

The Solution should have the ability to aggregate exceptions data to spot patterns that may not be visible at the level of an individual participant.

The FPN is centralized with comprehensive data recording, allowing for detailed logs to capture exception data and other events. The logs can be manually and/or programatically analyzed to spot exceptions that are not visible to the individual participant. The log data is also sent to specialized processes at the FPN operations center that automatically graphs inbound
information so that exceptions can be monitored, identified, diagnosed, and corrected before individual participants are aware of exceptions.

The FPN is flexible and allows for many types of information and events to be captured, analyzed and graphed, including but not limited to, successful authentications, failed attempts to authenticate, successful transfers, failed transfer attempts, and many other types of events.

### Part C, Section 3: Safety and Security

<table>
<thead>
<tr>
<th>Criteria Name</th>
<th>Section &amp; Consideration Name</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety and Security</td>
<td>S.1, Risk Management</td>
<td>✔</td>
<td>100</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.2, Payer Authorization</td>
<td>✔</td>
<td>104</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.3, Payment Finality</td>
<td>✔</td>
<td>106</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.4, Settlement Approach</td>
<td>✔</td>
<td>107</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.5, Handling Disputed Payments</td>
<td></td>
<td>108</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.6, Fraud Information Sharing</td>
<td></td>
<td>110</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.7, Security Controls</td>
<td>✔</td>
<td>113</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.8, Resiliency</td>
<td>✔</td>
<td>122</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.9, End User Data Protection</td>
<td></td>
<td>124</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.10, End User/Provider Authentication</td>
<td></td>
<td>126</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.11, Participation Requirements</td>
<td></td>
<td>130</td>
</tr>
</tbody>
</table>

**S.1, Risk Management**

Risk management means that the Solution should have a framework (rules, policies and procedures) to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, and other risks across the end-to-end payments process.
S.1.1, Risk of Unexpected Application of Laws

The Solution’s risk management framework should address the risk of an unexpected application of a law or regulation.

Because the FPN is principle-based and developed using Internet standards, it has an architectural design that is adaptable to unexpected application of a law or regulation. For example, the FPN has the ability to adapt rules applicable to payment addresses in the GDS based on where the individual who controls the payment address is domiciled. The FPN also employs a payment workflow that allows individual steps of the transfer process to be customized for the application of law and regulation.

The FPN’s risk management framework also proposes that the Federal Reserve perform the following functions:

- Cryptographically sign and issue Fed notes
- Control the Internet domain where the Fed notes are issued and made available to consumers and businesses
- Distribute Fed notes through depository institutions
- Regulate the payment system

Although not even the Federal Reserve can anticipate how the courts may interpret or apply a specific law, the Federal Reserve is the primary regulator and will have the ability to analyze related payment information as it considers how regulations are to be drafted that may impact the FPN.

S.1.2, Settlement Risks

The Solution’s risk management framework should address risks related to the solution’s Settlement approach (see S.4).

The FPN’s risk management framework is based on the use of Fed notes for transfers that mimic the pattern of use for physical Fed notes. As with the use of physical Fed notes, there is no lag time between transfer and finality when payments are completed using digital Fed notes. Inter-provider settlement risk is eliminated because there are no intermediate providers when the Fed notes are accepted for deposit by a provider. The use of digital Fed notes also eliminates credit, liquidity, and settlement risk for all providers.

S.1.3, Operational Risks

The Solution’s risk management framework should address operational risks related to deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events (see S.8).

The FPN’s risk management framework will address the operational risk of deficiencies in information systems, deficiencies in internal processes, human errors, management failures or disruptions from external events with a comprehensive documented set of policies, procedures, practices, information systems design, network design, application design, and cryptosystem design that coordinate and function together to optimally balance systems costs, performance and expectations of the market and to adjust to a changing threat environment.
The parties responsible to achieve the optimal balance of the risk management framework include the Federal Reserve as the primary regulator, the Governing Organization, other vendors that perform additional functions to operate the services (including hardware and software providers), independent system reviewers and auditors, and other stakeholders in the value delivery chain.

S.1.4, Risk of Unauthorized or Fraudulent Payments
The solution's risk management framework should address the risk of unauthorized, fraudulent (including first-, second- and third-party fraud, and fraud in the inducement), or erroneous payments (see S.3, S.5, S.7, and S.10).

S.1.4.1, First-Party Fraud

First-party fraud related to chargebacks
The FPN’s risk management framework addresses the risks of fraudulent payments for instances of first-party fraud related to chargebacks.

- The FPN uses push payments exclusively instead of allowing the Payee to pull from the Payer’s payment address.
- Because the FPN does not need to share sensitive information (e.g., account numbers, card numbers, personal information, etc.) with the Payee, laws surrounding chargebacks are not invoked by the FPN.
- The FPN requires the Payer to sign each payment order.
- The FPN requires the Payer to reconfirm at the time of payment, that the payment order once executed is immediate, final and irrevocable by the Payer’s depository institution or regulated non-bank provider, the Federal Reserve as the issuer of the digital banknotes, the Governing Organization, and other stakeholders in the transfer.

First-party fraud involving an account established using synthetic identity
The FPN intentionally allows all consumers to freely obtain a payment addresses in the Global Services Directory without verifying a government issued identity for the following reasons:

- The FPN is provided as a public service freely available to all consumers and businesses with limited abilities to send and receive Fed notes.
- The FPN allows individuals to establish a payment address without confirming identity but addresses synthetic identity theft through additional identity verification that is required for higher value payment addresses and transfers.
- The FPN offers the Federal Reserve and the Governing Organization ability to regulate and oversee the function and operation of the system including the ability to analyze the source, destination and amount for all transfers in lieu of identity verification for every individual.

S.1.4.2, Second-Party Fraud
The FPN’s risk management framework addresses the risk of second-party fraud (e.g., a trusted party with access to a person's credentials completes and signs a payment order) by implementing the following:

- The FPN supports optional two-factor authentication that when activated assures that the individual authenticating is also in current possession of protected secret information (i.e., token generated from biometric information).
Faster Payments Network Solution Proposal

- The FPN’s payment order dialog supports reverifying the presence and possession of the secret information (i.e., token generated from biometric information) before the Payer’s signature will be applied to the payment order.

S.1.4.3, Third-Party Fraud

The FPN’s risk management framework addresses the following instances of third-party fraud:

- A transfer or attempted transfer by an unknown entity that is not authorized by the Payer to use the payment address to make a purchase.
- An attempt to use the payment instrument to initiate funds transfers.
- An attempt to use the payment instrument to withdraw cash from the payment address.

The FPN reduces the risk of a transfer or attempted transfer by an unknown, unauthorized entity by the following mechanisms:

- Payment instruments, the Fed notes, are affixed to a single, authoritative Internet domain controlled by the Federal Reserve, where all transfers (i.e., possession updates) executed by the system are centrally recorded. Consequently, holders of the Fed notes are educated about the trustworthiness of the payment system at a universally trusted location on the Internet (e.g., fednotes.org).
- In contrast to checks or payment cards, only known individuals with valid Payer credentials are authorized to access the Payer’s payment address and to sign payment orders. (Payees are not permitted to access a Payer’s payment address to initiate or sign payment orders.)
- Requiring the Payer to re-authenticate to the system before the payment order is signed depending on the value of the transfer.
- Payment orders with instructions for the transfer of Fed notes are push-only payments.
- Because Payers do not share credentials with Payees, the FPN eliminates the risk of an attempt to use the payment instruments to initiate funds transfer by Payees.
- A Payer’s credentials are required for the Payer to deposit the Fed notes into an account with a depository institution or regulated non-bank provider.

S.1.4.4, Fraud in the Inducement

The FPN’s risk management framework at present does not address fraud in the inducement. Although the FPN does not specifically offer technological improvements to address fraud in the inducement or to mediate on behalf of individuals (i.e., consumers) that claim to be victims of fraud in the inducement, individuals are not without redress. Individuals are encouraged to report claims to organizations that are established to handle such claims, including the Better Business Bureau, the Federal Trade Commission, the Consumer Financial Protection Bureau, and the individual’s state attorney general. Rules may be adopted that block individuals or entities that are convicted of fraud from participating in the system.

S.1.4.5, Erroneous Payments

The FPN’s risk management framework includes the following features to reduce the risk of a Payer initiating erroneous payments:
Faster Payments Network Solution Proposal

- It allows Payees to link verifiable payment address aliases that are known and understood by Payers (e.g., cell phone number, email address, social media profile) to their primary payment address.
- It allows the Payer to select a Payee from a contact list created and managed by the Payer (e.g., mobile phone contact list, email address contact list, etc.).
- The FPN stores a list of frequent payment addresses that the Payer has sent to so that when the Payer searches for a payment address, the entries for frequent payment addresses are easy to see.
- The FPN makes the Payer financially responsible for payment orders initiated in error.

### S.1.5, Incentives

The Solution’s risk management framework should include incentives (i.e., positive, negative, financial, or non-financial) to operators and providers to address and contain risks they pose to other Participants.

The FPN provides similar incentives and balance risks to participants and providers as the physical cash system. Because risks are balanced among participants, including depository institutions and regulated non-bank providers, special incentives are not required.

### S.1.6, Periodic Reviews and Updates

The Solution’s risk management framework should be subjected to periodic review and update.

The FPN’s Governing Organization is responsible to see that the FPN’s risk management framework is subject to periodic review and update (see G.1.4). The Governing Organization will see that, for example, the following reviews and audits are conducted periodically:

- Independent compliance reviews
- Participant contract reviews
- Reviews of policies, procedures and operations
- Security reviews
- Applicable and appropriate information system audits and accreditations

### S.2, Payer Authorization

Payer authorization, including preauthorization, means that the Solution should require payments to be initiated only with the explicit and informed consent (see U.3.2) of the Payer to the Payer’s depository institution or regulated non-bank provider.

### S.2.1, Authorization of Providers

The Solution should require the Payer to authorize to their depository institution/regulated non-bank provider concurrently with payment initiation for each payment, unless the payment is preauthorized prior to payment initiation.

The FPN uses digital Fed notes to transfer value from Payer to Payee; consequently, as with the transfer of value from Payer to Payee when physical Fed notes are used, the Payer is not required to receive authorization from their depository institution or regulated non-bank provider when initiating a payment. The FPN enables the secure, efficient transfer of value directly from Payer to Payee in Fed notes. The Payer’s depository institution or regulated non-bank provider is a
stakeholder in the transfer only when the Payer is making a deposit to an account with a depository institution or regulated non-bank provider.

**S.2.2, Preauthorization of Providers**

If the Solution allows preauthorization, it should enable the Payer to preauthorize the Payer’s depository institution or regulated non-bank provider to make one or more payments based on defined parameters, as relevant to those payments (e.g., account from which funds are drawn, Payee, frequency, time and date, amount, amount limits, duration of authorization, etc.). The set of preauthorizations made by the Payer should subsequently be visible to the Payer.

The FPN supports preauthorizations and refers to preauthorizations as payment codes; however, because the FPN uses Fed notes to transfer value directly from the Payer to the Payee, the FPN does not need to preauthorize with the Payer’s depository institution or regulated non-bank provider to make one or more payments based on defined parameters relevant to preauthorized payments.

The FPN’s payment code capability allows the Payer to see the payment code, to configure certain parameters related to the payment code (e.g., the payable party, currency, amount and expiration for the payment code), to optionally skip the payment, or to retract (i.e., cancel) the payment code. The configuration of payment codes is handled directly between the system and the Payer without the need to communicate with the Payer’s depository institution or regulated non-bank provider.

The FPN will only initiate a transfer as instructed by the Payer’s payment code when the Payer is in possession of sufficient funds in Fed notes for the value of the payment code verified by the recipient. While payment codes can operate for all targeted use cases, currently they are configured for use with person-to-business and business-to-business transactions.

View a demonstration of how payment codes are used for preauthorization.

**S.2.3, Cancellation of Preauthorization**

If the Solution allows preauthorization, it should enable easy and timely cancellation of any preauthorization or change of preauthorization parameters by the Payer.

The FPN allows easy and timely modification or cancellation of payment codes by the Payer. The FPN allows the Payer to view all payment codes and select from the existing payment codes to make modifications as necessary or cancel a payment code. All changes to payment codes are updated in real time, and the effect on the payment code is immediate.

View how the FPN allows payment codes to be modified or cancelled.
S.3, Payment Finality

Payment Finality means that the solution should define a point in time after which a payment is Irrevocable. (See S.5 regarding protections to Payers for fraudulent or erroneous payments.)

S.3.1, Verification of Good Funds

The Solution should require the Payer’s depository institution or regulated non-bank provider to approve each payment following payment initiation to assure the Payer’s account has good funds.

This consideration statement presupposes that a solution will require a depository and/or regulated non-bank provider to approve each payment following initiation to assure the Payer’s account has good funds. However, today physical transfers using Fed notes are conducted directly between a Payer and Payee without requiring the Payer’s depository institution or regulated non-bank provider to approve each payment. Correspondingly, the FPN allows a Payer in possession of digital Fed notes (representing known good funds) to assign possession of the Fed notes to the Payee without requiring the Payer’s depository institution or regulated non-bank provider to approve each transfer.

S.3.2, Clarification of Irrevocability

The Solution should architecturally enable, and have rules and a supporting legal framework that clarifies, exactly when the payment becomes irrevocable, but this should be after good funds approval and no later than when funds are made available to the Payee. The exact point of irrevocability should be easily understood by and visible to the payee (see F.5).

The FPN’s rules (see L.2) and legal framework (see L.1) are based on the transfer of physical Fed notes. The FPN’s display of the confirmation page after the execution of the payment order is the step in the payment process when the transfer becomes irrevocable. The FPN will complete the transfer of value before the Payer and Payee are notified, so notification to the Payee and Payer is also an indication that the transfer of value is final.

Although transfer of value is final when either the payment confirmation page is displayed or the Payer and Payee receive notification, the FPN allows a Payee to voluntarily return the value to the Payer at any time.

S.3.3, Consumer Protection Regulations

The Solution should provide mechanisms and processes to protect or compensate the Payer in the event that the payment is disputed and to comply with relevant consumer protection regulations, including Regulation E (see S.5 and L.1).

The FPN does not limit the legal rights of a Payer to dispute payments. However, the FPN’s legal framework (see L.1) establishes that the payment is final once the system completes the execution of the Payer’s digitally signed payment order. The FPN does not provide a Payer the right to dispute payments through the Federal Reserve (i.e., the issuer of the digital Fed notes), the Governing Organization or the Payer’s depository institution or regulated non-bank provider.
S.4, Settlement Approach

Settlement approach means the solution should, by its design and rules, determine when and how depository institutions and regulated non-bank providers settle their obligations between each other; it should also determine the mechanisms to proactively manage any related credit and liquidity risks.

S.4.1, Settlement Timing and Process

The Solution’s rules should define when and how depository institutions and regulated non-bank providers settle obligations to one another arising from end user payments (e.g., Real-time gross Settlement, deferred net Settlement, frequency of Settlement, hours of Settlement operation, etc.). The solution’s participation requirements should be designed to ensure that compliant depository institutions and regulated non-bank providers have the operational, financial, and legal capacity to fulfill their obligations, including to other providers, on a timely basis. Where a depository institution or regulated non-bank provider settles on behalf of others, it may be appropriate for the solution to impose additional requirements to ensure that the settler has the financial and operational capacity to do so.

The FPN’s design and rules do not cause settlement obligations to arise between depository institutions or regulated non-bank providers because of end user payments; consequently, depository institutions and regulated non-bank providers are not subject to additional or special operational, financial, or legal responsibilities because of their participation in the FPN. Like the transfer of physical Fed notes between a Payer and Payee, the FPN’s transfer of digital Fed notes between Payer and Payee does not give rise to settlement obligations between a depository institution and/or regulated non-bank providers. The FPN enables the immediate, real-time transfer of digital Fed notes directly from the Payer to the Payee.

S.4.2, Management of Lag Between Transactions and Settlement

The Solution’s risk management framework should have an approach to proactively manage inter-Provider credit and liquidity risk exposures arising from any lag between transaction finality and inter-provider Settlement and to ensure that credit exposures to each provider can be fully covered. Any special credit and liquidity risk considerations for a FPN that is available to end users on a 24x7x365 basis should be addressed.

The FPN’s risk management framework eliminates the lag between transaction finality and inter-provider Settlement; consequently, providers are not subject to inter-provider credit or liquidity risk exposures. Although the FPN is designed to operate continuously without interruption (i.e., 24x7x365), at no time does the FPN pose special credit or liquidity considerations for providers.

S.4.3, Credit and Liquidity Risk

The solution should either enable settlement in central bank money or minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money for the inter-provider settlement process.

The FPN’s settlement approach is to settle all transfers immediately and finally in Fed notes, completely eliminating credit and liquidity risk. The FPN’s settlement approach is patterned after the settlement approach used by printed Fed notes and coins, where settlement is complete when the Fed notes change possession from the Payer to the Payee.
S.5, Handling Disputed Payments

Handling disputed payments means that the solution should have rules, processes and timeframes for effectively addressing unauthorized, fraudulent, erroneous, or otherwise disputed payments. For each of these, the solution should have an appropriate allocation of liability among, and substantive liability limits for, all parties, including the Payer, the Payee, and the providers involved in the payment. (See S.3 regarding payment Finality).

S.5.1, Preventing Disputed Payments & Holding Rule Violators Accountable

The Solution’s rules should include requirements, processes and timeframes for addressing unauthorized, fraudulent, erroneous, or otherwise disputed payments, as well as mechanisms to hold rule violators accountable. For example, the solution should include mechanisms to block funds availability if an unauthorized, fraudulent, or erroneous payment is reasonably identified by the receiving depository institution or regulated non-bank provider prior to payment finality.

The FPN’s rules address potential unauthorized, fraudulent, erroneous, or otherwise disputed payments and hold potential rule violators accountable by requiring the following:

- All payments orders that include the transfer of Fed notes are executed by the system as push-only payments.
- All payment orders must be authorized and digitally signed by the Payer using the Payer’s private key prior to the system’s execution of the payment order.
- Unless otherwise specified in the rules, the Payer is required to waive the right to have disputes mediated by the Federal Reserve, the Federal Reserve Banks, the Governing Organization, or other stakeholders or non-stakeholders (e.g., the Payer’s depository institution or regulated non-bank provider) of the transfer.
- The Payer is accountable and financially responsible for the submission of incorrect or erroneous information on a signed and submitted payment order that is irrevocably executed by the FPN.
- The FPN prevents the Payer from spending more than s/he holds in Fed notes.

S.5.2, Communicating How Providers Comply with Consumer Protection Laws

The Solution should make clear how a consumer Payer’s provider can comply with consumer protection laws related to error resolution and fraudulent or unauthorized payments; this requirement does not apply to first-party fraud, which is covered in S.1.4.

The FPN does not define a consumer Payer’s provider. The FPN does define a Payer, a Payee and a provider; however, the FPN does not define a consumer’s depository institution or regulated non-bank provider as a consumer’s Payer provider; consequently, depository institutions and regulated non-bank providers continue to comply with consumer protection laws related to error resolution and fraudulent or unauthorized payments as they do now. The FPN holds the Payer accountable and financially responsible for errors submitted by the Payer on payment orders. The FPN’s requirements and framework protect the Payer’s provider by requiring and enabling the direct transfer of known good funds for every payment authorized by the Payer.
S.5.3, Ability to Request Return of Funds

The Solution should provide mechanisms for any party to the transaction to request prompt voluntary return of funds from the Payee, or the return of funds as required by law.

The FPN provides mechanisms for Payees to voluntarily, and without cost, return funds to the Payer. The FPN allows only the Payer to request the return of funds from the Payee within the FPN. Any party or stakeholder to the transfer can request a prompt voluntary return of funds from the Payee on behalf of the Payer; however, for the targeted use cases, the stakeholders in the transfer are the Payer, the Payee and the Federal Reserve. Unless a change is specifically requested or supported by the Federal Reserve, the rules and software features do not enable the Federal Reserve as the issuer of the Fed notes to make a request to the Payee for prompt voluntarily return the funds on behalf of the Payer. The FPN’s rules and features support the Payee's return of funds as required by law.

S.5.4, Business and Government Protection

The Solution should adopt an approach, including the delineation of roles, responsibilities and liability allocation, which reasonably protects business and government Payers against losses related to fraud or errors and adheres to applicable laws or regulations.

The FPN adopts an approach to liability allocation that reasonably protects business and government Payers against losses related to fraud or errors by implementing best practice processes and procedures (i.e., software features) that help reduce errors and assist in the prevention of fraud. The FPN specifically reduces the possibility of first-, second-, and third-party fraud and fraud in the inducement as follows:

S.5.4.1, First-Party and Third-Party Fraud

The FPN eliminates the possibility of first-party and third-party fraud by limiting transfers of Fed notes to push-only payments, and requiring that all payment orders are digitally signed by individuals using valid credentials that ensure their authorization to act on behalf of the organization.

S.5.4.2, Second-Party Fraud and Fraud in the Inducement

The FPN assists business and government Payers with the reduction of errors and prevention of second-party fraud and fraud in the inducement as follows:

- The FPN requires that authorized individuals, acting with their own valid credentials, enroll the business, manage the business, and digitally sign and authorize all payment orders.

- Managers must use their own valid credentials to approve or delegate to other individuals the authority to perform certain system functions (e.g., sign payment orders, review and/or audit transfer history, and schedule payments).

---

48 An in-system request from the Payer to the Payee to voluntarily return funds is a feature to be added.
Faster Payments Network Solution Proposal

- The system records, logs and tracks all activity within the context of the business payment address by user (e.g., manager or delegate).
- Transfers that involve Fed notes are limited to push-only payments.
- There is an option to require each payment order to have two digital signatures before submission to the system for execution.
- User sessions are locked after an inactivity period lapses (e.g., 5 minutes).

In addition, the FPN’s rules hold the business and/or government Payer accountable and financially responsible for errors on digitally signed payment orders executed by the system. The FPN also adheres to applicable laws and regulations (see L.1).

S.5.5, Protecting Payers from Fraud Loss

The Solution should adopt an approach, including the delineation of roles, responsibilities and liability allocation, which reasonably protects consumer Payers against losses related to fraud or errors and adheres to applicable laws or regulations (e.g., Regulation E and Regulation Z).

The FPN adopts an approach to liability allocation that reasonably protects consumer Payers against losses related to fraud and errors by implementing the following:

- Transfers of Fed notes are limited to push-only payments.
- All payment orders are signed by the consumer Payer using his or her own token before the system transfers Fed notes. (The FPN rules and functions do not permit a Payee to sign a payment order that includes the transfer of Fed notes on behalf of a consumer Payer.)
- A consumer Payer can send payments to a known Payee using a primary payment address alias (e.g., cell phone, email address, social media profile, etc.).
- A consumer Payer can request a voluntary return of the funds for an erroneous transfer.

The FPN’s rules hold consumer Payers accountable and financially responsible for errors on signed payment orders executed by the system. The FPN also adheres to applicable laws and regulations (see L.1).

S.6, Fraud Information Sharing

Fraud information sharing means that the Solution should require and facilitate timely and frequent sharing of information among all providers, operators and regulators to help them manage, monitor, and mitigate fraud and evolving threats.

S.6.1, Managing and Monitoring Fraud

The Solution should require the sharing of information to facilitate managing and monitoring fraud (e.g., patterns suggestive of risk, known instances of fraud, known vulnerabilities, the significance of the information, and effective mitigation techniques). Personally identifiable information should be excluded from information sharing (see S.9 and L.4).

The FPN streamlines the process of sharing information to facilitate managing and monitoring fraud by centrally collecting and aggregating information for all transfers under the Internet domain where the Fed notes are issued (e.g., fednotes.net). The FPN maintains a central permission system to allow it to control access to features and information. Information related to changes of possession of Fed notes is available to stakeholders involved in the transfer. The central collection of information also makes it possible for the FPN to do the following:
Faster Payments Network Solution Proposal

- Analyze transfers in real-time to ensure compliance with regulation and law
- Quickly identify and flag patterns suggestive of risk
- Identify known instances of fraud
- Keep mitigation techniques up to date and current with a changing threat environment
- Appropriately limit the sharing of personally identifiable information

The FPN’s rules are embedded in the computer code that executes all transfers; consequently, a Payer is not able to submit a payment order that would cause a transfer to be executed in violation of the rules, regulations or laws. For example, if a consumer Payer holds $500 and he tries to submit a payment order for more than $500, he will receive a message indicating that the transfer exceeds the amount of funds he holds and the payment cannot be completed.

The FPN is a central repository of information collected under the web domain controlled by the Federal Reserve. Information about participants (e.g., individuals and businesses, financial institutions, etc.) is logged, reviewed and continuously monitored, allowing patterns suggestive of risk to be identified and evaluated from a system-wide view.

The FPN’s system-wide view also means that fraud and fraud patterns can be identified in real-time and, once known, mitigated. To keep mitigation techniques up to date in a changing threat environment, the FPN will be subject to regulation updated at all system levels.

Finally, the FPN has a roles-based permission system that controls the appropriate sharing of contextual data, transfer data, and personally identifiable information. For example, the FPN allows an individual to set up a business payment address. Once the business is set up, the individual that created the business uses his or her personal credentials to manage and access information related to business transfers. The manager has authority to grant permissions to other individuals who can then also manage the business payment address. Each manager uses his or her own user credentials to authenticate to the system. Activity performed by a manager of the business payment address, such as transfer of Fed notes to another business, is logged against the user credentials performing the action.

**S.6.2, Data Sharing**

The Solution should describe how data owned by entities other than providers and operators would be aggregated, managed and protected for purposes of fraud information sharing.

The FPN is centralized and ownership of the data is governed specifically by the participation agreements for providers, individuals and businesses (see L.1). Because the FPN is centralized and each entity must agree to terms and conditions of the participation agreement, information is aggregated under the domain controlled by the Federal Reserve, managed by the Governing Organization, and protected and shared for the purposes of fraud according to the rules.

The FPN manages the sharing of information for fraud purposes through a roles-based permission system. For example, unless otherwise filtered by the rules, providers will have visibility for all transfers related to distribution and deposit to an account with the provider. Providers will not have visibility for person-to-person transfers; however, the provider may have visibility for transfers between entities when the provider is in the role of Payer or Payee for the transfer. Thus, the provider’s responsibilities for sharing of information, protecting information or fraud reporting can be specifically limited to transfers that involve the provider.
S.6.3, Fraud Monitoring

The Solution should facilitate information sharing that supports real-time and ex-post management and monitoring of fraud, and provides timely updates and alerts.

The FPN’s information sharing is facilitated by a selection of standard information sharing formats (e.g., xml, json, webhooks) that allow participants to receive reports and monitor information in real time. For example, the FPN allows a provider with membership in an organization like Financial Services Information Sharing Analysis Center (FS-ISAC) to stream information for real-time analysis and alerting.

S.6.4, Ease of Implementation

The Solution’s information sharing mechanisms should be easy to implement, update and maintain.

The FPN’s information sharing mechanisms are based on standard data interchange formats and protocols (e.g., xml, json, csv, rss, html). The FPN’s sharing mechanisms include activity feeds available to participants and integrators. Activity feeds can be formatted as web pages, as widgets that can be included in a web page, or other open, distributed, publish/subscribe communications protocol including Atom, JSON and PubSubHubbub. The FPN’s sharing mechanisms allow various types of data (e.g., html, text, pictures, audio and video) to be shared. Because the FPN’s sharing mechanisms are based on standard data interchange formats and up to date Internet communication protocols, they are easy to implement, easy to update, and easy to maintain.

View how the FPN allows participants to create activity feeds.

S.6.5, Differentiated Access to Content

The Solution’s information sharing mechanisms should support differentiated access to content based on the roles and responsibilities of each operator, provider and regulator.

The FPN’s design includes a role-based permission system that supports different access to content or information based on individual roles. For example, an individual can be granted permission as the manager of a business payment address in addition to controlling his own payment address. Once granted permission as a manager of the business payment address, the individual’s user credentials inherit the permission associated with managing the business payment address. All of the individual’s business payment address activity is associated with the individual’s role as the manager and personal credentials. Roles-based permissions also allow individuals to be removed, updated or changed without impacting the payment activity associated with the business payment address. The roles-based permissions also allow more than one individual to be in a specific role (e.g., a business can have many managers).

The FPN also has access control for the supported types of activity feeds (See S.6.4). Access to activity feeds are restricted by a secret key that is embedded in the subscription URL, and
Internet Protocol (IP) address. Appropriate users have the capability to manage (i.e., view and change) the secret keys used to access activity feeds.

**S.6.6, Central Repository**

The Solution’s information sharing mechanisms may include a central authoritative trusted repository to perform functions such as storage and aggregation of the information.

The FPN’s design and information sharing mechanisms (i.e., roles-based permission system and activity feeds) are centralized, and authoritative (i.e., controlled by the Federal Reserve), meeting the requirement for storage and aggregation of information. For example, in the targeted use case of person-to-person transfers, the Payer may be authenticated to the system using a web browser, while the Payee authenticates through an integrator’s mobile wallet application (e.g., Apple wallet, Google wallet). Regardless of how an entity connects to the system, information about the Payer’s payment order and the Payee’s receipt of the payment is centrally recorded and viewable by the Payer, the Payee, and stakeholders of the transfer.

As another example, a business participant may want to stream activity to another application. The manager of the business payment address can configure the activity feed and provide the URL endpoint to the receiving application, at which point the listening or receiving application will receive up-to-date, real-time information as specified in the configuration.

**S.6.7, Discovering Patterns of Fraud**

The Solution should have the ability to aggregate fraud information to spot patterns that may not be visible at the level of an individual participant.

The FPN is centralized; consequently, all information related to transfer and contextual data is subject to both manual and automated analysis to identify fraud and fraud patterns at every system level.

**S.7, Security Controls**

Security controls means that the solution has layered and robust technical, access, operational, procedural, and managerial controls to address and foster security, including but not limited to the integrity and protection of confidential, private and sensitive data.

**S.7.1, Provide Strong Technical Access Components and Controls**

The Solution should provide strong technical access components and controls, including (a) identity verification and access management, (b) data encryption in transit and at rest, (c) data quality and integrity controls, (d) data breach and detection, (e) layered security controls, and (f) components and controls that leverage and are consistent with industry standards.

**S.7.1.1, Strong Identity Verification and Access Management.**

The Solution should provide strong identity verification and access management.

The FPN integrates with external identity service providers and/or hardware tokens that provide strong, asymmetric digital signatures. The system employs digital signatures both for authentication and signed payment orders.
The FPN also employs a username and password or passphrase pair as a method to verify an end user’s identity. The FPN’s default is single-factor authentication, but it also allows for end users to select optional two-factor authentication. End users may select from various supported methods of second-factor authentication including one-time passwords using a secondary communication channel (e.g., sms/text message), one-time passwords using a separate application (e.g., VIP Access from Symantec, Google Authenticator) or a device that displays the one-time password (e.g., Security token or card), hardware key using PKI (e.g., Yubikey) and biometrics using mobile devices.

The FPN may require an end user to activate multi-factor authentication as required by some business processes and security features (e.g., a business may require all managers to use multi-factor authentication to sign a payment order). The FPN has a password policy that is updated from time to time. The password policy requires end users to have a password of minimum length (e.g., 8 characters) and include a combination of alpha characters, numbers, special characters and spaces. The FPN also has a real-time password strength meter to give end users immediate feedback on the strength of the end user’s selected password or passphrase.

Another aspect of the FPN’s access management system is to permit the end user to set an optional personal identification number (“PIN”). The PIN is only used to resume an end user’s session after it has expired (see S.7.1.5 and S.10). The PIN does not replace the username and password/passphrase or multi-factor credential.

The FPN’s access management system allows end users to reset passwords and passphrases using the primary communication channel established during enrollment (e.g., email address or mobile device). The password/passphrase reset is fully automated and may require the end user to provide additional verification (e.g., predetermined challenge response questions set at the time of enrollment).

The FPN’s access management system is roles- and permission-based. End users can be assigned to various roles within the system and inherit permissions associated with those roles. Roles and permissions are also set in context within the system. For example, an end user may be a manager of both a business payment address and an individual payment address. The access management system requires the end user to set the appropriate context before being able to perform specific functions in that context. Another example of roles includes the ability for a payment address to function as a distribution, redemption, or settlement payment address for a particular brand of closed-loop cash within a specific closed-loop network on the system.

**S.7.1.2, Strong Data Encryption**

The Solution should provide strong data encryption in-transit and at-rest.

The FPN encrypts data both in transit and at rest.

The FPN encrypts data in transit as follows:
Faster Payments Network Solution Proposal

- Data in transit between servers and clients is encrypted using Secure Hypertext Transport Protocol (HTTPS) using Transport Layer Security (TLS) consistent with the guidelines published by NIST.\textsuperscript{49}
- Data in transit between servers is encrypted using TLS encryption.
- The FPN uses a Virtual Private Network (VPN) to secure the communications for some administrative processes and services.

The FPN encrypts data at rest as follows:

- Certain records at rest in the database are hashed (e.g., passwords) using secure hashing algorithms consistent with guidelines published by NIST.\textsuperscript{50}
- All data at rest on hard drives are encrypted using algorithms based on Advanced Encryption Standard (“AES”), a NIST-adopted standard.

\textit{S.7.1.3, Data Quality Controls}


| The Solution should provide data quality and integrity controls. |

The FPN ensures the highest degree of data quality by adhering to the following data quality characteristics:\textsuperscript{51}

- Accuracy
- Access
- Consistency and precision
- Timeliness

The FPN’s ability to ensure adherence is the crucial data characteristic listed above that achieves an overall high degree of data integrity, trustworthiness, and public confidence.

\textbf{Accuracy}

The FPN achieves a high degree of data accuracy by ensuring the following:

- Cryptographically signed and issued Fed notes, once created, are not altered, deleted or destroyed.
- Each Fed note is assigned an immutable, publically viewable URL under a domain controlled by the Federal Reserve.
- Each Fed note is assigned an immutable standard monetary value (e.g., $.01 to $100).
- Each Fed note is assigned a single possession attribute.
- The system allows one and only one holder of any individual Fed note at any given moment in time.

\textsuperscript{50} Secure Hashing, Computer Security Division, Computer Security Resource Center, National Institute of Standards and Technology.
\textsuperscript{51} Understanding Data Integrity v. Data Quality, Care Communications Blog.
The system allows the Fed notes’ possession attribute to be updated only by (a) the current holder, (b) individuals authorized by the current holder (i.e., in the role of manager in the case of a business) after the individual has successfully authenticated to the system, or (c) officials executing a court order.

The system executes and records the request to update the possession attribute only after receiving a signed payment order from the current holder or person authorized to act on behalf of the current holder.

**Access**

The FPN achieves a high degree of data access by ensuring the following:

- Members of the public and all participants can freely access, view and validate the authenticity of Fed notes using a standard web browser and the Fed notes’ public key. Authentication is not required for this function.
- Individuals meeting the minimum participation requirements can create a free payment address and hold Fed notes.
- Businesses meeting the minimum participation requirements can create a free payment address and hold Fed notes.
- Participants holding Fed notes are free to transfer the Fed notes to others (i.e., individuals or businesses) in accordance to the rules, applicable regulations, and law.
- End users with a payment address are free to see that the system has executed the transfer of Fed notes according to their signed payment order.

**Consistency and Precision**

The FPN operates with a high degree of data consistency by keeping the requirements for submitting a payment order simple (e.g., source of funds, destination of funds, and amount) and executing all payment order instructions precisely without error.

**Timeliness**

The FPN achieves a high degree of data timeliness by executing instructions and completing all transfers in real time, with appropriate notifications to the Payer and Payee. The FPN’s use workflows allows the FPN to execute a series of steps that may include a pause in the execution of the payment order’s instructions for a certain period of time or until the occurrence of an event (e.g., enrollment by a payee responding to an invitation).

**S.7.1.4, Data Breaches**

The Solution should provide measures to prevent and detect data breaches.

Data breach prevention includes developing appropriate policies and policy management practices as well as information security controls. Several groups share the responsibility for developing appropriate measures: the implementing team, the Federal Reserve as the controller

---

52 Source of funds explicitly means the payment address of the authenticated end user.
of the web domain, the Governing Organization, and other Parties (i.e., hardware and software vendors) that may be involved in the implementation of the FPN. Data loss prevention is a complex issue and an ongoing concern; therefore, the approach to data breach prevention needs to be comprehensive and designed for the scale of operation.

The FPN has applied standard tools to detect data breaches but proposes that the implementation rely on technologies from existing best-in-class providers of data breach detection technology.

S.7.1.5, Layered Security Controls

The Solution should provide layered security controls (e.g., The Open Systems Interconnect, OSI).

The different layers of security include physical, data link, network, transport, session, and application. The controls included in the FPN for each of these layers are outlined below.

Physical

Physical layer security controls are comprehensive and relate the security of all physical elements of the environment where the FPN is operated, including placement and protection of network patch panels, protection of cable trays and cables (e.g., ethernet, fiber, etc.), power interfaces, power backup, power generators, power supply, air conditioning, air circulation and ventilation, raised flooring, etc. The implementation team, the Governing Organization, the Federal Reserve, and other vendors will develop comprehensive security controls for protection of the FPN’s physical layer to prevent intrusion, service interruption, and possible compromise. The FPN does not currently provide specific guidelines to improve physical layer security but rather relies on the expertise of a core group of experienced engineers and professionals to assist the implementation team with initial physical layer security controls.

Data Link

Data link layer security includes defending against threats and attacks that can be executed at the FPN’s physical and logical network layer. The Implementation team, the Governing Organization, the Federal Reserve, and key vendors will be responsible for overseeing and implementing a network design to defend and prevent attacks at the data link layer. The FPN does not currently provide specific guidelines that improve data link layer security but rather relies on and utilizes the industry’s best products and configuration strategies to defend against security threats at the data link layer.

Network

Network layer security includes defending against a number of possible and evolving attacks primarily within the Internet Protocol (IP) packet. The FPN records IP information received, so it can be used in transfer analysis to identify possible red flags or AML issues; however, the FPN does not offer technological enhancements to improve network layer security. The Implementation team, the Governing Organization, the Federal Reserve and key vendors will have responsibility to utilize best-of-breed network layer security products offered by industry vendors to mitigate network layer attacks.

Transport

The FPN uses Transmission Control Protocol (TCP) at the transport layer. Transport layer security includes defending against threats and attacks that exploit TCP. The FPN does not offer
technological enhancements to improve the transport layer security but rather will rely on the Implementation team, the Governing Organization, the Federal Reserve, and key vendors to provide transport layer security products and strategies to mitigate transport layer attacks.

**Session**

The FPN’s session layer security is used to establish confidence in participant identities and mitigates session layer threats by implementing the following:

- Requiring the participant to establish authentication credentials (i.e., secret information) during enrollment using either a cryptographic hardware token, identity management provider, email verification, or mobile phone verification.
- Encrypting secret information in transit and at rest.
- Requiring the participant to prove the possession of or knowledge of the secret information (e.g., password, token, biometric) issued during enrollment before establishing secure sessions.
- Varying the participant’s authentication identity assurance level based on the following: (a) the total value the participant can hold (e.g., a participant who can hold more than USD $2500 must use two-factor authentication), (b) the amount the participant can send, and (c) the roles associated with the participant (e.g., an individual who also serves as the manager of a business payment address must use two-factor authentication).
- Requiring the participant to prove identity using documentary sources when higher levels of identity assurance are required for authentication (e.g., establishing a link between a payment address and an account with a depository institution that has verified the participant’s documentary sources).
- Allowing the participant to establish verified links to the payment address at other sites that offer non-documentary evidence of identity or even proof of identity (e.g., social media sites, blogs, identity service providers or verifiers).
- Requiring the participant to enter a CAPTCHA after three or five failed authentication attempts.
- Locking a participant’s access for a specified period of time (e.g., 24 hours) after a certain number of failed attempts (e.g., ten), except when the participant authenticates using a hardware access token or identity services provider.

The FPN implements session layer security in accordance with guidance from National Institute of Standards and Technology.\(^53\)

**Application**

The FPN implements Transport Layer Security (TLS) using the TLS 1.2 protocol specification designed to prevent message tampering, eavesdropping, and message forgery. The FPN uses TLS for communications between servers and clients. TLS is also used for message communications between modules (e.g., front end, transfer server, message queue).

The application layer will be subject to many security threats. Security threats at the application layer will be ongoing and intensifying; consequently, security controls must also be ongoing and coordinated from the top down, including the entire technical staff of software engineers, quality assurance, network engineers, hardware engineers, and security experts. The importance of security controls at the application layer cannot be understated, and ongoing development of security controls will be required for production deployment. To provide necessary protection, security controls must be coordinated and comprehensive across all layers.

The participants who use a hardware key and/or identity service providers reduce the attack surface at the application layer.

**S.7.1.6, Complying with Industry Standards**

The Solution should provide components and controls that leverage and are consistent with industry standards (e.g., NIST, ISO, ANSI).

The FPN’s components and controls use and are consistent with the following Internet Standards and protocols: (a) Internet Protocol using Transmission Control Protocol (TCP/IP), (b) Domain Name System (DNS), (c) Secure Hypertext Transport Protocol (HTTPS) with Transport Layer Security (TLS), (d) Hypertext Markup Language (HTML), (e) Javascript, (f) Cascading Style Sheets (CSS), (g) Secure Hashing Algorithms (e.g., SHA-1, SHA-2, SHA-3), and Digital Signatures (e.g., DSA, RSA, ECDSA). The implementation team, the Governing Organization, and independent auditors and reviewers will ensure information systems components and controls are consistent with industry standards and NIST recommendations.

**S.7.2, Operational Controls**

The Solution should provide strong operational and procedural components and controls, including (a) data retention and disposal controls, (b) physical security, (c) operations security, monitoring, and incident response, and (d) communications and network security.

**S.7.2.1, Data Retention and Disposal**

The Solution should provide strong data retention and disposal controls.

The implementation team, working with the Governing Organization and with oversight and approval by the Federal Reserve, will develop data retention and disposal policies consistent with

---

56 HTML5 published by W3C.
57 Cascading Style Sheets published by W3C.
58 Javascript Web APIs published by W3C.
60 Digital Signatures, Computer Security Division, Computer Security Resource Center, National Institute of Standards and Technology.
recommendations by NIST,\textsuperscript{61} current best practices, regulations\textsuperscript{62} and law. The Governing Organization will ensure that data is retained and disposed of according to policy and procedure.

The FPN provides strong data retention controls by implementing technology that assists in retaining including hot replication, offsite backups, and quick failover. For example, if a database fails, the FPN can switch to a different replica of the same database. Another example is the disposal of old hard drives. Because drives are encrypted (see S.7.1.2, Data encryption at rest), deleting the first few blocks of a partition is sufficient to make the entire contents of the drive impossible to read.

\textbf{S.7.2.2, Physical Security}

The Solution should operate in an environment with strong physical (environmental) security.

The Implementation Team, working with the Governing Organization and with oversight and approval by the Federal Reserve, will develop physical security policies and procedures that are consistent with recommendations by NIST,\textsuperscript{63} other standards organizations, federal laws, executive orders, and state-of-the-art practices. The policies and procedures will specify the design of a physical security system that will be dependent on technologies working together as an integrated system to ensure security at all physical threat levels (e.g., doors, windows, vents, hardware) and against intrusions. Physical security requires a multiple-disciplinary approach that considers all aspects of the physical environment, including locations of data centers, redundancy of utilities, power backup, power generation, design of walls, floors, and ceilings, location of entry points, exit doors, stairwells, elevators, the use of surveillance systems, visitor screening and armed security guards. The policies and procedures require a rigorous certification and accreditation process on various components to ensure the overall integrity of the physical security system.

\textbf{S.7.2.3, Operational Security}

The Solution should provide strong operational security, monitoring, and incident response.

Operational security is comprehensive and includes physical security (see S.7.1.5, Layered Security Controls), monitoring and surveillance. To assist in operational security, monitoring and incident response, the FPN is built using an industry standard automated deployment system. The deployment system applies global changes and can report unauthorized changes. The deployment system also configures a monitoring system that alerts administrators when a system component needs attention. The FPN provides a global system log that includes messages and warnings for detecting possible attacks.

\textsuperscript{61} An example of an applicable NIST is Special Publication 800-92, “Guide to Computer Security Log Management.”

\textsuperscript{62} Examples of related Federal Regulations include Sarbanes-Oxley Act of 2002 (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act of 1996 (HIPPA) and Payment Card Industry Data Security Standard (PCI DSS).

S.7.2.4, Communications and Network Security

The Solution should provide communications and network security.

The FPN employs TLS for all communication with participants and for internal message communication (see S.7.1.5, Layered Security Controls). The FPN is regularly subjected to industry standard software tests and assessments to identify known weaknesses. The FPN is also regularly subjected to independent penetration tests and vulnerability scans. Security control at other layers will be determined and implemented by the implementation team and the Governing Organization in accordance with industry standard practices and guidance.

S.7.3, Managerial Policies and Oversight

The Solution should have strong managerial policies and oversight that (a) integrate with existing risk management processes, (b) are adaptable to enterprise-level security architectures, (c) comply with provider-specific governance and risk management attributes, and (d) motivate investments by all parties to collectively and continuously improve the security of each transaction.

S.7.3.1, Risk Management

The Solution’s managerial policies and oversight should integrate with existing risk management processes.

The FPN’s managerial policies and oversight integrate with existing risk management processes by following the model of the physical cash system and preserving important attributes including the following:

- Preserving the role of the Federal Reserve as issuer of the Fed notes and regulator of the payment system
- Preserving the role of depository institutions as distributors and depositories of the Fed notes
- Minimizing and limiting new oversight responsibilities for depository institutions and changes to existing risk management process (e.g., AML, BSA, KYC, CIP, etc)
- Centralizing the responsibility for rule making and governance in a membership-based organization whose membership is representative of the broad diversity of participants in the payment system (e.g., individuals, businesses of varying sizes, depository institutions, regulated non-bank providers, third-party processors, developers, integrators, and federal, state and municipal government users)
- Centralizing the responsibility for regulatory compliance of the payment system with the Governing Organization

S.7.3.2, Enterprise Security

The Solution’s managerial policies and oversight should be adaptable to enterprise-level security architectures.

The FPN’s implementation team and the Governing Organization with oversight of the Federal Reserve, will provide strong managerial policies and oversight that are adaptable to enterprise-level security architectures. The executive team of the Governing Organization will create, translate, and communicate vision and strategy into effective policies and procedures that allow the Governing Organization and the payment system to adapt to market demands, adhere to
principles of the payment system, and protect the payment system from an expanding threat environment.

**S.7.3.3, Provider-Specific Attributes**

The Solution’s managerial policies and oversight should comply with provider-specific governance and risk management attributes (see S.1).

The FPN’s Governing Organization has the primary responsibility for governance and risk management. The FPN also allows providers to continue with existing day-to-day governance and risk management programs. The implementation of the FPN does not immediately impose new governance responsibilities on providers.

**S.7.3.4, Continuous Improvement**

The Solution’s managerial policies and oversight should motivate investments by all parties to collectively and continuously improve the security of each transaction.

The FPN’s design and architecture limits and centralizes the security responsibility to a few key stakeholders, primarily the Governing Organization and key vendors providing products or services to assist in securing and protecting the FPN from an increasing threat environment. The Federal Reserve, in coordination with the Governing Organization, will approve managerial policies to ensure proper motivation to invest in and continuously improve security. The FPN’s business model will provide the financial resources necessary for continuous improvement in security as necessary for operation in an expanding threat environment.

**S.8, Resiliency**

Resiliency means that the Solution has mechanisms and systems to ensure high levels of end-to-end availability and reliability under normal and stressed operating conditions.

**S.8.1, Target Metrics**

The Solution should define its target availability metrics and describe its approach to ensure those metrics can be achieved.

The FPN targets high availability (i.e., five nines). The FPN’s approach to high availability is the separation of stateless and stateful processes. Most processes are stateless because stateless processes are easier to scale. All front ends are stateless, while databases and messages queues are stateful. To scale the stateful components, the FPN employs messaging, replication, and sharding. The messaging architecture allows the FPN to avoid scaling problems associated with distributed locking and distributed transactions. Because the FPN will become highly important to the function of the US economy, it will need excess capacity and strategies, mechanisms and technology to mitigate and deal with DDoS attacks, bot traffic and other types of cyber attacks. The implementation team will work with the Governing Organization, the Federal Reserve, and various vendors that provide detection and mitigation for the FPN.

**S.8.2, Business Continuity**

The Solution should have business continuity and disaster recovery plans to ensure timely recovery and resumption of critical services in the event of an outage or a cyber-attack.
The implementation team and Governing Organization, working with the Federal Reserve and other vendors, will develop and implement comprehensive business continuity and disaster recovery policy and plans to ensure five nines of reliability and uptime. The executive team of the Governing Organization will have responsibility for drafting the written continuity and recovery policy and overseeing adherence to policy in day-to-day operations. The executive team will ensure that business continuity and disaster recovery policy and plans are developed in accordance with NIST recommendations. The continuity and recovery plans are part of a comprehensive, ongoing emergency preparedness effort by the Governing Organization, the Federal Reserve, and other key vendors that are integrated into the fabric and culture of the Governing Organization.

**S.8.3, Avoiding Systemic Risks**

The Solution should have mechanisms to minimize the chance that an adverse solution-related event will cause other market participants to fail to meet their obligations (i.e., trigger systemic risk).

The following mechanisms within the FPN are designed to minimize the chance that adverse FPN-related events will cause other market participants to fail to meet their obligations:

- The Federal Reserve is required to (a) be the issuer of the Fed notes, (b) control the supply of the Fed notes and (b) act as the redeemer of last resort.
- Fed notes are affixed to a globally recognized and trusted domain under the control of the Federal Reserve.
- The FPN maintains real-time, accurate and complete possession records for all Fed notes.
- The FPN eliminates credit and liquidity risk by eliminating lag time between delivery of good funds in Fed notes and final Settlement.
- The implementation of the FPN very effectively satisfies all the effectiveness criteria related to safety and security, legal framework, and governance.

**S.8.4, Resources for Business Continuity**

The Solution should demonstrate that sufficient resources are devoted to business continuity and resiliency.

The Governing Organization will ensure that sufficient resources are devoted to continuity and resiliency. The Governing Organization will obtain the necessary financial resources to support continuity and resiliency plans by executing the business plan that includes revenue from membership fees paid by voting members, fees from brand cash distribution agreements with businesses issuing brand cash, and fees from premium features for businesses. The executive team, led by the Chief Information Officer of the Governing Organization, will ensure that staffing levels are maintained to fulfill regular continuity plan training, testing, exercises and maintenance.

---

Faster Payments Network Solution Proposal

**S.8.5, Contingency Testing**

The Solution should conduct regular contingency testing across all operators and providers of its end-to-end systems.

The FPN has a distributed design and architecture, but the components are not distributed among providers; consequently, the FPN’s Governing Organization, working in coordination with the Federal Reserve and key applicable vendors (e.g., hardware, software, etc.), will develop a comprehensive payment system contingency plan that is consistent with NIST recommendations. The Governing Organization’s executive team oversees the entire contingency planning process and will approve the contingency planning policy and procedures, conduct business impact analysis, and perform contingency training, contingency plan testing and exercise, and contingency plan updates and maintenance.

**S.9, End User Data Protection**

End user data protection means that the Solution should have controls and mechanisms to prevent the unintended exposure of end-user data. End user data, both digital and physical, should be protected in transit and at rest, before, during, and after a transaction, so that it is not exposed erroneously.

**S.9.1, Protecting Sensitive Information**

The Solution should require that all operators and providers through the end-to-end payments process have robust controls and mechanisms to protect sensitive information (including for end users), as appropriate to their roles (see also L.4).

The FPN’s implementation of the GDS (see S.9.2) eliminates the need to require providers to have special provisions for robust controls and mechanisms through the end-to-end payment process to protect sensitive information. The FPN’s robust controls and mechanisms implemented in the GDS are applicable and available to all Payers, Payees, depository institutions, regulated non-bank providers, end users and participants.

**S.9.2, Avoiding Unnecessary Disclosure of Sensitive Information**

The Solution should have controls and mechanisms to protect sensitive information needed for account setup, transaction setup, and problem resolution from unnecessary disclosure. For example, the Payer and Payee should not need to know each other’s account numbers or other sensitive information to initiate or receive the payment.

The FPN’s implementation of the GDS eliminates the need to unnecessarily disclose sensitive information as follows:

---

• Sensitive information can be mapped to public, semi-public or private URLs anchored in the context of the Internet domain controlled by the Federal Reserve (the “authorized domain”).
• URLs can be substituted when needed in the processes for mapped account information (e.g., checking, savings, payment card accounts, etc.).
• It is possible to strictly control the use of the URL within the context of the authorized domain.
• URLs are rendered useless when use of the URL is attempted outside the context of the authorized domain.

The FPN is a system of addresses, not accounts. The FPN does not compete with depository institutions and regulated non-bank providers for deposits or deposit accounts; consequently, all deposit accounts are opened by end users through an account opening processes that is separate from the FPN, and procedures are controlled by providers outside the context of the FPN’s Internet domain.

In this solution proposal, transaction setup is referred to as a payment order. At a minimum, a payment order requires the following elements of information:

• Source payment address (i.e., may only be authorized by the current holder of the Fed notes after authenticating to the system by entering valid credentials)
• Destination payment address or an alias mapped thereto (e.g., cell phone number, email address, social media profile address etc.)
• Currency and amount to be transferred

The payment order minimally requires the Payer to enter a Payee’s primary payment address or an alias (e.g., cell phone number, email address, social media profile address etc.) mapped by the Payee to the Payee’s public payment address.

The use of the GDS protects sensitive information and eliminates the need for Payers and Payees to exchange depository account information.

View a demonstration of how a Payer sends a payment knowing only the Payee’s payment address.

The FPN allows the end user to control and share information related to enrollment (i.e., payment address setup). For example, an end user may choose to optionally upload a photo, address information, link to profiles on other social media sites, or create a custom name for the primary payment address. The FPN’s participant agreement and privacy policy protects the Federal Reserve and the Governing Organization when an end user voluntarily discloses or links to personally identifiable information.

S.9.3, Protecting Information Needed to Process Payments

The Solution should have controls and mechanisms to protect any sensitive information that is needed to process and complete a payment. For example, the Payer and Payee should not see one another’s account numbers or other sensitive information at any point throughout the end-to-end payment process.
Faster Payments Network Solution Proposal

The FPN protects sensitive information that is needed to process a payment by implementing a GDS with public and/or private addresses (i.e., URLs) that can take the place of the sensitive information needed to process a payment. Furthermore, all URLs in the GDS are electronically anchored to the web domain controlled by the Federal Reserve and are invalid when an attempt is made to use the URL outside the context of the authorized domain.

For example, an individual can create a link (i.e., URL) to a checking account. After the payment system establishes that the individual is the owner of the checking account, the payment system creates a unique URL in the GDS to substitute for the routing number and account number. Afterward, the unique URL is used by the FPN in place of the account number.

As another example, a unique URL can be created that links to the account number, expiration date, and other sensitive payment card account information, without actually storing the payment card information inside the GDS. Then the URL representing the payment card (e.g., credit, debit, or prepaid) can be used for certain target use cases (e.g., person-to-business, and business-to-business).

View a demonstration of how the system allows individuals to link to a checking account.

S.10. End User/Provider Authentication

End user/provider authentication means the Solution should require robust identification and verification for enrolling and transacting with end users and providers.

S.10.1, Framework

The Solution should define a robust framework that operators and providers will use to authenticate providers and end users to the system.

The FPN advocates adherence to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Guiding Principles for end user identity and authentication. End users utilize secure, efficient, easy to use and interoperable identity credentials to access the system. The NSTIC principles provide end users with credentials to online services that promote confidence, privacy, choice and innovation.

The FPN does not make a distinction between end users or providers for the purposes of authentication. Authentication credentials are issued to an individual, and individuals are assigned permissions based on their organizational roles (e.g., CFO, Audit, Accounting) and in the context of the system (e.g., manager of a business, closed-loop network administrator, etc.).

The FPN supports authentication methods that include identity service providers, passwords set by end users, personal identification numbers, and physical devices with cryptographic keys and biometric identification, such as smartphones and key fobs.

**S.10.2, Ensuring Payments Reach Payees**

The Solution should have robust mechanisms to ensure the payment is destined to reach the intended Payee at the intended Payee account. For example, the solution might (a) require the payee’s provider to explicitly communicate acceptance of a payment before finalizing the transaction, (b) provide a mechanism for sending a pre-notification or “test message” to help confirm the identity of the Payee and to validate the existence of the Payee’s account, and/or (c) require monitoring for payment anomalies (see S.7.2).

The FPN has the following mechanisms to ensure the payment reaches the Payee’s intended account: (a) the GDS, (b) payment codes, and (c) test transfers.

**S.10.2.1, The Global Directory Service**

The FPN supports several kinds of payment destinations, which are referred to as addresses. One type of address is the primary payment address for participating entities (e.g., fedcash.com/walmart, fedcash.com/bankofamerica, fedcash.com/joescafe). The primary payment address is a payment system endpoint that is associated with an end user (or end users in the case of a business payment address) and is expressly under the end user’s control. It functions as a sort of digital wallet for the end user.

Another type of address on the payment system is an alias to the primary payment address. After a primary payment address is active on the payment system, an end user in control of the payment address can add an alias to the primary payment address. A primary payment address alias must be verified before becoming active; however, after it has been verified, a Payer can use the primary payment address alias as a substitute for the primary payment address to send money.

For example, when enrolling, an individual is required to prove that he or she is in control of at least one acceptable primary communication channel (e.g., cell phone or email) before the enrollment process can finalize and activate the primary payment address. To verify the individual is in control of the email address provided at enrollment, the system sends an email message containing a unique, short-lived link. The end user’s ability to open the email and click the short-lived link is confirmation to the payment system that the individual is in control of the email address. Upon completion of the email verification process, the payment system adds the email address as a primary payment address alias for the end user’s payment address.

In another example, the end user can enroll and provide his or her cell phone number as the primary communication channel. The system will then go through a routine to validate that the

---

67 Examples of valid primary payment addresses include the following: 1) email addresses, 2) cell phone numbers, and 3) social media profile addresses (e.g., facebook.com/toddaadland, twitter.com/seanrodriguez, linkedin.com/in/sethruden, plus.google.com/+bradleywilkes).
individual is in control of the cell phone number before finalizing enrollment and activating the primary payment address. After the cell phone number has been verified, the Payment System adds the cell phone number as a primary payment address alias to the end user’s payment address.

The FPN capability for personal and business end users to set up aliases to a primary payment address is scalable, flexible, extensible and designed according to web standards. The addressing scheme supports a variety of devices (e.g., ATM, printers, vending machines, rental bikes, kiosks, etc.) to be aliased to a primary payment address. For example, a business that owns vending machines can create an alias for each of its vending machines. Then a Payer can make a purchase using Fed notes at each of the vending machines. The payment for the purchase at the vending machine is routed to the business’s payment address and includes data to specify the vending machine where the payment was made. As another example, a university can create payment aliases for printers and copiers so that students can pay for copies with Fed notes. Many other alias types are possible using the addressing scheme.

S.10.2.2, Payment Codes
When activated by the Payee, payment codes can be used by the Payer to conduct test transfers. The Payer can generate a payment code and provide it to the Payee to ensure that the payment will reach the intended recipient.

S.10.2.3, Test Transfers
The FPN makes it possible for the Payer to transfer a small amount of money (e.g., $.01) to the Payee to confirm that payment is destined to reach the intended Payee.

S.10.3, Industry Standards
The Solution should align with regulatory guidance (e.g., FFIEC) and industry standards (e.g., ANSI, ISO, W3C, etc.) for end-user authentication.

The FPN’s end-user authentication model aligns with the following regulatory guidance and industry standards:

- Electronic Authentication Guideline
- The National Strategy for Trusted Identities in Cyberspace
- The FIDO Alliance
- The OAuth 2.0 Authorization Framework

---

68 Electronic Authentication Guideline, NIST Special Publications 800-63-2, National Institute of Standards and Technology.
70 The FIDO Alliance.
The Solution should apply strong end-user authentication controls across all delivery channels and may vary the authentication procedure based on the risk-weighting of a given transaction.

The FPN has strong authentication controls across delivery channels, including third-party applications using the API (see S.10.5). The FPN supports varying the authentication procedure based on the following:

- Total value that may be held
- Amount of a payment order
- Whether or not the individual is a manager of a business that requires multi-factor authentication when the individual is acting on behalf of the business
- Resumption of a session after an activity timeout

The FPN supports requiring an individual to use multi-factor authentication when (a) the individual’s payment address is approved to hold large sums of Fed notes, and (b) the individual is a manager of a business that requires multi-factor authentication, and the individual is acting on behalf of the business.

The FPN makes it convenient for end users to reauthenticate after a session times out by asking the end user to enter a PIN to resume the session. The FPN supports varying authentication procedures based on the risk-weighting of a given transfer.

The Solution should enable the end user to be authenticated initially to the solution itself (prior to multiple transactions) and should also require providers to reauthenticate end users based on the risk-weighting of a transaction.

The FPN enables end users to authenticate to the system using an identity service provider, cryptographic hardware token, or a password/passphrase established by the end user at enrollment. The FPN proves identity of the end user by having the end user enter secret information. An end user can establish an optional Personal Identification Number (PIN) that can be used by the end user to resume a session after an activity timeout.

The FPN’s application program interface (API) adheres to the OAuth 2.0 Authorization Framework\(^72\) (OAuth2), a standard proposed by the Internet Engineering Task Force (IETF) that allows end users to grant limited permissions to a published application. The published application is issued a limited attribute access token different from the end user’s authentication credential when permission is granted to the published application by the end user. Separating the end user’s credentials from the published application’s access token adds a layer of protection to the authentication model. The FPN implements and adheres to OAuth2 to provide strong security for the API authentication model. The FPN’s API authentication model provides the following benefits:

\(^{72}\) The OAuth 2.0 Authorization Framework, Request for Comments: 6749, Internet Engineering Task Force (IETF).
• Provides a sandbox separate from production for third-parties to develop applications
• Allows the Governing Organization to control from within the system the publication and release of third-party applications and their authorization end-points (e.g., “fednotes.com/app/exxonios”) to end users
• Requires third-party applications to be certified before the application can be released and made public for end users
• Eliminates the need for third-party applications to store end user credentials, 
• Allows end users to limit the third-party application’s permissions to specific features in the end user’s payment address
• Allows end users to revoke a specific third-party application’s access to the end user’s payment address without revoking access for all third-party applications and without requiring the end user to change authentication credentials
• Provides a separate third-party application token refresh end-point (e.g., “fednotes.com/token/refresh”) to allow a third-party application to refresh the access token by prompting the end user to enter a PIN

OAuth2 is a newer authentication model that addresses problems of earlier client/server authentication models, such as OAuth 1.0.

The FPN’s design does vary the end user authentication requirements based on an individual’s permissions in the FPN (e.g., the manager of a business may be required to authenticate using two-factor authentication), the value that can be held in a payment address, and/or the value of a transfer.

S.10.6, Adopting and Decommissioning Authentication Models

The Solution should be able to adopt new and decommission old authentication models based on the evolving threat landscape.

The FPN’s Governing Organization is responsible to see that the FPN keeps pace with industry standards and requirements for new end user and API authentication models. The adoption of new end user or API authentication models will be achieved by the Governing Organization obtaining a consensus vote from the membership of the governing body to adopt new authentication models. Similarly, the Governing Organization will obtain a consensus vote to decommission old authentication models unless there is a determination that the old authentication model is a threat to security of the system, in which case the rules permit the Governing Organization to act quickly to mitigate security threats.

S.11, Participation Requirements

Participation requirements means that the Solution should establish and monitor compliance with transparent requisites that providers must meet on an ongoing basis as appropriate to their roles in the solution.

S.11.1, Participation Requirements for Providers

The Solution’s participation requirements should be adequate to ensure that all providers adhere to the FPN rules and requirements relevant to their role, including those related to security, resiliency, anti-money laundering/know your customer, and data privacy/integrity protocols. See also criteria S.5-S.10.
The FPN’s participation agreement for providers will be adequate to ensure that all providers adhere to the FPN’s rules and requirements relevant to their roles by having the participation agreement drafted by legal counsel with full understanding of the system, the system’s rules, and the provider’s roles and responsibilities. The participation agreement will also be reviewed by counsel representing providers collectively to ensure that it is balanced before implementation. The participation agreement for providers, like the participation agreement for other entities (e.g., individuals and businesses), will also be subject to a periodic review and update to appropriately adjust to changes in rules (i.e., software code), procedures, roles and responsibilities, and the threat environment. Unless determined otherwise, legal counsel participating on the implementation team has responsibility to draft the initial version of the provider’s participation agreement.

**S.11.2, Ensuring Providers’ Ability to Fulfill Obligations**

The Solution’s participation requirements should be adequate to ensure that all compliant depository institutions and regulated non-bank providers have the operational, financial, and legal capacity to fulfill their obligations, including to other providers, on a timely basis (see S.4).

Other than the requirements and responsibilities associated with a depository institution’s role as a distributor of digital Fed notes, the FPN does not require special participant requirements for providers but rather utilizes the existing regulatory regime (e.g., Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Financial Institution and Money Service Business regulators at the state level) to ensure that providers have the operational, financial and legal capacity to fulfill their obligations.

**S.11.3, Monitoring Compliance**

The Solution should have processes to regularly monitor and ensure compliance by all providers against these requirements.

The FPN’s Governing Organization regularly monitors and ensures compliance to the participation requirements for all participants, including providers. The FPN seeks to implement many of the participation requirements in the software code of the payment system to minimize the need for external monitoring and compliance review of participants.
### Part C, Section 4: Speed (Fast)

<table>
<thead>
<tr>
<th>Criteria Name</th>
<th>Section &amp; Consideration Name</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed (Fast)</td>
<td>F.1, Fast Approval</td>
<td>✔</td>
<td>132</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.2, Fast Clearing</td>
<td>✔</td>
<td>132</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.3, Fast Availability of Good Funds</td>
<td>✔</td>
<td>132</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.4, Fast Settlement</td>
<td>✔</td>
<td>133</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.5, Prompt Visibility of Payment Status</td>
<td>✔</td>
<td>134</td>
</tr>
</tbody>
</table>

#### F.1, Fast Approval

Fast approval means that the Solution should require and enable the Payer’s depository institution or regulated non-bank provider to assure good funds for each payment in a timely manner, as indicated by the effectiveness scale below.

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes for the targeted use cases. Each Fed note represents good funds. The possession of the Fed notes is transferred from the Payer to the Payee immediately when payments are made. Consequently, payments do not require approval of the Payer’s depository institution or regulated non-bank provider.

#### F.2, Fast Clearing

Fast clearing means that the Solution should require and enable the Payer’s and Payee’s depository institution or regulated non-bank provider to exchange payment information in a timely manner, as indicated by the effectiveness scale below.

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes for the targeted use cases. Payments completed with Fed notes do not require the Payer’s and Payee’s depository institution or regulated non-bank provider to exchange payment information. The FPN requires the Payer and Payee to exchange payment information and does so in real time.

#### F.3, Fast Availability of Good Funds

Fast availability of good funds to the Payee means that the Solution should require and enable funds and contextual data, as appropriate (see U.4, Contextual Data Capability), to be received by the Payee, such that the funds can be withdrawn or transferred in a timely manner, as indicated by the effectiveness scale below.

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes for the targeted use cases. Contextual data is available to the Payer and Payee for all Fed notes that are or have been in their possession. Funds are available for withdrawal or transfer by the Payee immediately.
after the FPN completes execution of the instructions on the Payer’s submitted payment order. The FPN executes all submitted payment orders in real-time and displays a confirmation page to the Payer indicating that the transfer is complete. Both the Payer and Payee also receive notification following the completion of the transfer.

View a demonstration of how funds can be withdrawn or transferred immediately after receipt.

F.4, Fast Settlement

Fast settlement means that the Solution should require and enable obligations between the Payer’s and Payee’s depository institution or regulated non-bank provider to be discharged in a timely manner, as indicated below.

F.4.1, Management of Credit and Liquidity Risks

The Solution should have an approach to manage credit and liquidity risk exposures arising from any lag between transaction finality to the Payee and inter-provider settlement, including, for example, if a Solution is available to end users on a 24x7x365 basis but inter-provider Settlement is not (see S.4).

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes for the targeted use cases. Because the possession attribute of the Fed notes is updated and possession is transferred from the Payer to the Payee immediately when the FPN executes the Payer’s signed and submitted payment order, there is no lag in settlement, and no credit and liquidity risk for providers.

F.4.2, Time Zone Considerations

Any special considerations for handling settlement between depository institutions or regulated non-bank providers located in different time zones should be addressed.

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes. Because the possession attribute of Fed notes is updated immediately, in real time there is no lag in settlement and impact for transfers that span different time zones.

F.4.3, Managing Deferred Settlement

The Solution may provide flexibility to the depository institution or regulated non-bank provider to determine the timing of settlement (e.g. the depository institution or regulated non-bank provider might choose immediate or deferred settlement) as long as the associated risks of deferred settlement are managed (see F.4.1).

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes. Like payment with physical Fed notes, payment with digital Fed notes does not require the depository institution or regulated non-bank provider to be involved in settlement or determine the timing of settlement. The possession attribute of the Fed notes is updated from the Payer to the Payee, immediately, in real time. The FPN also supports an option for the Payer to specify a time for the FPN to execute the submitted payment order. This feature gives the Payer the flexibility of
completing, signing and submitting the payment order but having the execution of the payment order deferred until a specified time.

F.5, Prompt Visibility of Payment Status

Prompt visibility of payment status means that the Solution should enable mechanisms by which both the Payer and the Payee can track the payment at various stages of the end-to-end payment process in a timely manner, as indicated by the effectiveness scale below.

F.5.1, Visibility for Payer

For the Payer, visibility should include when their payment has been approved (see F.1, Fast Approval on page 132), their Account has been debited, and the Payee has received the funds in their Account for use.

The FPN’s use of Fed notes for payment mimics the use of physical Fed notes. The FPN provides full transparency to both the Payer and Payee of transfer information and contextual data for all steps of the transfer process in real time. The Payer or Payee can view the details of a transfer that include the sequential steps and stages the FPN performed to complete the transfer.

F.5.2, Visibility for the Payee

For the Payee, visibility should include when the payment has been approved (see F.1, Fast Approval on page 132) and when funds become available for use in their Account.

Because the FPN processes Fed note payments in real time, funds are available to the Payee for use or transfer immediately when the FPN completes executing the Payer’s submitted payment order.

View how the FPN allows for prompt visibility of payment status.

---

73 The deferment of execution of a payment order is a feature to be included at implementation.
Part C, Section 5: Legal Framework

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>Section &amp; Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.1, Legal Framework</td>
<td>✔</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.2, Payment System Rules</td>
<td>✔</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.3, Consumer Protections</td>
<td>✔</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.4, Data Privacy</td>
<td>✔</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.5, Intellectual Property</td>
<td>✔</td>
</tr>
</tbody>
</table>

**L.1, Legal Framework**

Legal framework means that the Solution should describe the legal sources which will govern the operation of the solution and/or impose any compliance obligations on the Solution or end users, and describe any contemplated changes or additions to existing laws necessary to support the Solution.

Although the technical details of the Faster Payments Network (FPN) are detailed elsewhere in this proposal, it is useful to reiterate here the essential elements of the FPN:

- The Board of Governors of the Federal Reserve System (the “Federal Reserve” or “Fed”) would issue digital banknotes (referred to elsewhere in this proposal as Fed notes), each of which is represented by an Internet protocol (IP) address controlled by the Fed.
- Definitive record ownership of each such digital banknote would be controlled and with the owner’s permission publicly displayed by the Fed.
- Each digital banknote would be cryptographically “signed” by the Fed using “asymmetric cryptography,” also known as “public key cryptography.”
- “Transfer” of digital banknotes would be achieved via the exchange of cryptographically signed messages among the Fed, the payer, and the payee, whereby the payer, as holder of a digital banknote, would assign the banknote to the payee using his/her private key. A payer would issue transfer instructions to the Fed, as the controller of the Internet domain associated with each digital banknote and custodian of the transfer record, with a copy to the designated payee. The transfer would be effective upon the Fed’s update of its records, and the execution of the transfer would be confirmed by the Fed to both parties, again in cryptographically signed messages.
- The Fed (or a party contracted by the Fed) would act as the root level “certificate authority” (CA) for the system, thereby controlling who is able to receive and transact in digital banknotes.
The digital banknotes would constitute “legal tender” to the same degree as paper Federal Reserve notes and coins issued under the authority of the U.S. Department of the Treasury (“Treasury”).

Transfer of digital banknotes on the records of the Fed would be final and irrevocable.

In sum, the Federal Reserve would perform at least three (3) key functions in this model: (i) issuer of digital banknotes, (ii) CA for the public key infrastructure (PKI) that would support distribution and transfer of notes, and (iii) custodian of digital notes, including authentication of ownership and recording of ownership transfers. In addition, the Federal Reserve may wish to administer a Global Delivery Service (GDS) that enables users of the FPN to search for an individual’s public key, as described above, to facilitate cash payments between users. The GDS also could enable users to find additional information regarding potential counterparties (e.g., name, email address, public email certificates). The GDS would receive continuous data updates from the PKI and could be an authoritative source for PKI certification validation. The GDS would also be an authoritative source for certificate revocation lists and certificate authority certificates.

Upon issuance, each digital banknote will be signed with a private key controlled, managed and maintained exclusively by the Federal Reserve. The GDS will include a reference to the corresponding public key that allows the holder of the banknote to validate the authenticity of the banknote and its digital signature. The digital banknotes also will bear a Fed-assigned serial number and such other identifying marks as the Fed may determine, as with physical banknotes. Consistent with its role with respect to physical banknotes, the Fed should be the operator of the site in order to protect and enhance confidence in the digital banknotes and manage, maintain and ensure an adequate supply of digital banknotes as part of the overall money supply.

One of the strengths of the proposed FPN is its flexibility with respect to the role of depository financial institutions in the chain of distribution of digital banknotes. For example, the Fed could engage depository institutions to act as intermediaries with respect to the distribution of digital banknotes, similar to their role with respect to the distribution of existing Federal Reserve notes and the automated clearinghouse (ACH) and wire transfer systems (the “Bank Centric” model). In a Bank Centric model, the Fed would issue digital banknotes to eligible banks, directly or through the Federal Reserve Banks, and those banks would be authorized to redistribute the digital banknotes to customers who had satisfied anti-money laundering (AML) and Office of Foreign Assets Control (OFAC) screens. Moreover, the recipients of those digital banknotes would be able to transfer them only to persons (individuals and entities) whose identity had been validated in accordance with applicable AML and OFAC standards by banks authorized by the

Administration of the GDS, the “back-office” machinery necessary for authentication and recording, and numerous other aspects of the Faster Payments Network described herein, may be delegated to the Governing Organization (described elsewhere in this proposal) or a service provider as the Fed sees fit. Our intent is not to dictate whether or how the Fed may exercise its discretion to delegate operation of the various components of the FPN; rather, where the FPN contemplates operative concepts from the point of view of Fed action, it should be understood to refer to action by the Fed or its designee, and not to derogate from the Fed’s flexibility to delegate or otherwise involve the Governing Organization, its members, or other third parties as necessary or appropriate to provide the FPN.
Fed for that purpose. Only the banks participating in the FPN would be permitted to request the Fed (as CA) to issue key pairs to the validated recipient.

Alternatively, the Fed could determine to issue the digital banknotes directly to the public (the “Bank Light” model). Under the Bank Light model, the Fed would directly occupy a more prominent role with respect to all aspects of administration of the FPN, including by taking responsibility for validation of the identity for the recipients and transferees of digital banknotes. We believe that the Fed is more likely to select the Bank Centric model because it (i) is more consistent with the Fed’s current mode of operation, (ii) takes advantage of existing bank relationships with customers to avoid replication of customer identification programs (CIP) on persons whose identity has already been validated in connection with their existing bank accounts and (iii) avoids putting the Fed in the position having to undertake CIP tasks (beyond validating the eligible banks).

Finally, the Fed could undertake some combination of these two models, for example if the Fed determined that it, or the Federal Reserve Banks, should act as a direct distributor of last resort, or should provide a conduit for certain types of other non-bank distributors, such as broker-dealers. Another hybrid alternative, explored below, would allow for a multi-tiered holder base, segregated by the extent of bank CIP screening that a holder has undergone: holders who have not undergone full bank CIP would be subject to transaction limits (e.g., by amount or volume), which would not apply to holders who have undergone CIP and hold their digital banknotes in a deposit account. The FPN is sufficiently flexible to allow multiple tiers of transactional authorization determined by the Federal Reserve based on the level of identity validation performed or other factors.

In either model, security of the private key will be a critical issue. Security requirements could be mandated by the Fed, although it is recommended that only high-level standards be established (e.g., multi-factor authentication) so that the market is free to evolve the most effective security implementations.

L.1.1, Identifying Legal Sources

The Solution should identify relevant and applicable legal sources such as existing public sector laws, regulations, regulatory interpretations or rulings, court decisions and/or payment system rules that will apply to the payment system, end users, providers, Payers and Payees, and payments through the payment system.

L.1.1.2, Introduction

The Solution is intended to enable real-time payment over the Internet among all registered participants in the GDS. To that end, the objective is to have payment by digital banknotes mimic payment by paper money in terms of the effectiveness and finality of payment.75

75 It is also important to stress that the digital banknotes (Fed notes), like physical Federal Reserve notes, represent a direct claim against the United States, as distinguished from a claim on a bank deposit in an ACH or wire transfer.
We address below principles of law governing payment by physical Federal Reserve notes and explain how those principles could apply to digital banknotes under the solution. We begin by discussing the underlying authority of the Federal Reserve to issue digital banknotes. We then turn to certain fundamentals of the law of payment by physical legal tender, followed by an explanation of why these features also should apply to the law of payment by digital banknote as legal tender.

**L.1.1.3, Fed Notes Authorized by the Federal Reserve Act**

Digital banknotes should be treated as authorized by the Federal Reserve Act to the same extent as physical banknotes.

In its concrete form as a medium of exchange, physical currency consists today of coins and Federal Reserve notes. At present in the United States, coin issue is governed by Section 5111 of Title 31, U.S. Code (“Minting and issuing coins, medals, and numismatic items”), which provides that the Secretary of the Treasury (“Secretary”) “shall mint and issue coins described in section 5112 of this title in amounts the Secretary decides are necessary to meet the needs of the United States.” Section 5112 of Title 31 authorizes the familiar denominations of coin (penny, nickel, dime, quarter, half dollar and dollar) and the requirements of each in size and mass.

As for Federal Reserve note issuance, Section 16(1) of the Federal Reserve Act provides:

> “Issuance of Federal Reserve notes; nature of obligation; where redeemable”

Federal Reserve notes, to be issued at the discretion of the Board of Governors of the Federal Reserve System for the purpose of making advances to Federal Reserve banks through the Federal Reserve agents as hereinafter set forth and for no other purpose, are hereby authorized. The said notes shall be obligations of the United States and shall be receivable by all national and member banks and Federal Reserve banks and for all taxes, customs, and other public dues. They shall be redeemed in lawful money on demand at the Treasury Department of the United States, in the city of Washington, District of Columbia, or at any Federal Reserve bank.\(^76\)

Federal Reserve note denominations are provided in Section 8 of the Federal Reserve Act, but unlike with respect to coins, which may be issued “only” in the specific denominations and sizes, Federal Reserve notes are not expressly limited to the denominations stated.\(^77\) Specifically, the Secretary is directed to print Federal Reserve notes in denominations of “$1, $2, $5, $10, $20, $50, $100, $500, $1,000 $5,000, $10,000 as may be required to supply the Federal Reserve banks... in form and tenor as directed by the Secretary of the Treasury under the provisions of this Act and [bearing] the distinctive numbers of the several Federal Reserve banks through


\(^77\) Id. § 418.
which they are issued,” but the Secretary is not affirmatively limited to “only” those denominations.

Section 16(1) of the Federal Reserve Act is silent as to the medium in which Federal Reserve notes are to be issued. Accordingly, it may be argued that digital banknotes are encompassed within the general authority of Paragraph 1. This argument finds further support in the enactment in 2000 of the Electronic Signatures in Global and National Commerce Act (eSign Act), which provided among other things that, with respect to transactions in or affecting interstate or foreign commerce, “a signature, contract, or other record relating to such transaction may not be denied legal effect, validity or enforceability solely because it is in electronic form.” While payment by digital banknote may constitute more than a “signature, contract or other record,” the underlying intent of the eSign Act was to enable and encourage the development of electronic interstate commerce. Since Paragraph 1 does not prohibit the issuance of Federal Reserve notes in electronic form, it can be argued that it should not be read so narrowly in light of the clear policy choice of Congress to foster the development of electronic commerce.

Nonetheless, it is admittedly awkward to attempt to fit an electronic fiat currency regime within the terms of a statute written decades before the advent of the Internet. Indeed, while Paragraph 1 is silent as to the form of Federal Reserve notes, the remaining provisions of the Federal Reserve Act clearly contemplate paper currency. Because confidence in the basic underpinnings of a digital banknote system is essential to its operation, we offer in L.1.2, Addressing Gaps in the Legal Sources on page 142 proposed amendments to the Federal Reserve Act (“Proposed Amendments”) to leave no doubt on this point.

L.1.1.4, Fed Notes as “Legal Tender”

Assuming that digital banknotes are the legal equivalent of physical Federal Reserve notes under the Federal Reserve Act as written or amended, the “legal tender law” provides for the use of Federal Reserve notes in payment:

United States coins and currency (including Federal Reserve notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues. Foreign gold or silver coins are not legal tender for debts.

“Legal tender” is not further defined, but has been interpreted to mean money, that, at least in the absence of an agreement to the contrary, a debtor may offer and the creditor must accept in discharge of a debt. Furthermore, the Supreme Court has concluded definitively that Congress has the constitutional authority to make Federal Reserve notes legal tender.

---

80 See, e.g., Smith Mach. Co. v. Jenkins, 654 F.2d 693, 697 (10th Cir. 1981) (“payment of a debt may be made only in money unless the creditor consents to some other form of payment”) (New Mexico law); Woodhead Lumber Co. v. E.G. Niemann Invs., 22 P.2d 252, 253 (Cal. Ct. App. 1933) (“It is the general rule that nothing is to be considered
While the status of Federal Reserve notes as legal tender is a matter of Federal statute, the process of payment in cash is governed by common law, rather than statutory law or regulation. At common law, “payment” generally is broadly defined to mean the “[p]erformance of [a monetary] obligation by the delivery of money or some other valuable thing accepted in partial or full discharge of the obligation.” To constitute “payment,” a payer must actually or constructively deliver, or otherwise relinquish control of money, to a payee, with the intention or purpose on the part of the payer of extinguishing a debt or obligation, and the payee must manifest acceptance.

“Payment,” as described, must be distinguished from “tender.” “Tender is an offer to perform a condition or obligation coupled with the present ability of immediate performance, so that were it not for the refusal of cooperation by the party to whom tender is made, the condition or obligation would be immediately satisfied.” “‘Tender’ is an unconditional offer of payment consisting of the actual production of a sum not less than the amount due on a particular obligation.” However, “a tender of payment is not the equivalent of payment itself; technically, a tender of payment has not yet been accepted, while payment has.”

Thus, what separates “tender” and “payment” is the relinquishment of control of money by the payer, and the acceptance thereof by the payee. Money (or other legal tender) has long been held unique in that the payee who has accepted it in good faith may as the new holder treat the payer as payment in fact but that which is in truth such [payment in money] unless something else is expressly agreed to be received in its place.”

81 Juilliard v. Greenman (Legal Tender Cases) 110 U.S. 421, 450 (1884) (“We are irresistibly impelled to the conclusion that the impressing upon the Treasury notes of the United States the quality of being a legal tender in payment of private debts is an appropriate means, conducive and plainly adapted to the execution of the undoubted powers of Congress, consistent with the letter and spirit of the Constitution, and therefore, within the meaning of that instrument, ‘necessary and proper for carrying into execution the powers vested by this Constitution in the government of the United States.’”); Knox v. Lee (Legal Tender Cases) 79 U.S. (12 Wall.) 457, 542-45 (1871).
82 Black’s Law Dictionary (9th ed. 2009). Certainly however, “payment” may also be made by way of a gift or loan and be carried out by means of a transfer of monetary value or money fund rather than money in cash and coin.
83 See, e.g., U.S., to Use of Par-Lock Appliers of N.J. v. J.A.J. Constr. Co., 137 F.2d 584, 586 (3d Cir. 1943) (“It is quite elementary that when money is received by a creditor from a debtor, there must be, in order that the transaction may amount to a payment, (1) an intention of the delivering debtor that the transfer shall serve to extinguish, in whole or in part, the existing debt, and (2) a like intention on the part of the receiving creditor.”) Villafuerte v. Inter-Con Sec. Sys., Inc., 117 Cal. Rptr. 2d 916, 920 (Cal. App. Dep’t Super. Ct. 2002); Enriquillo Exp. & Imp., Inc. v. M.B.R. Indus., 733 So. 2d 1124, 1126 (Fla. Dist. Ct. App. 1999); First Heights Bank, FSB v. Gutierrez, 852 S.W.2d 596, 605 (Tex. App. 1993); French v. Detroit Fire & Marine Ins. Co., 38 So. 2d 165, 166-67 (La. Ct. App. 1948).
86 Williston, supra, § 72:27; see, e.g., Multach v. Adams, 418 So. 2d 1254, 1255 (Fla. Dist. Ct. App. 1982) (“The question of the effect of a tender of performance arises most frequently in the case of a unilateral money debt. In those cases, the tender of performance will not operate as a discharge of the debt nor does the refusal to accept the money tendered operate as a discharge of the debt.” (internal citations omitted) (quoting and citing 13-67 Corbin on Contracts § 67.6 (Joseph M. Perillo ed., 2015))).
as a valid transferor thereof, and the payee is also clothed with the power to further transfer it. Accordingly, payment with physical currency is made on the passage of possession in the money, coupled with the intent to transfer ownership therein, when the payee takes delivery, thereby manifesting the acceptance of the tender.

L.1.1.5, Application of Legal Principles to Payment in Digital Banknotes

If digital banknotes (Fed notes) qualify as Federal Reserve notes, as argued above, then they too would qualify as legal tender. As indicated above, the “legal tender law” applies to all Federal Reserve notes. Moreover, even if the Federal Reserve act must be modified to clarify the equivalence of digital banknotes and physical Federal Reserve notes, the “legal tender law” already applies more broadly to all forms of “currency”; Federal Reserve notes are just an example.

As shown above, substantial body of law has developed to accommodate payment in cash, covering tender, completion, and discharge of debt. At the same time, the proposed FPN involves digital banknotes that do not circulate in the traditional sense like physical notes; rather, control of the notes is determined with reference to an Internet domain at all times under the control of the Federal Reserve. The FPN operates by executing transfer instructions provided by the holders of the notes. The FPN’s execution of instructions from the payer updates the possession of the digital banknotes and thus changes control in them. Whether delivery of possession is evidenced by physical transfer of paper instruments or by irrevocable recording on a central ledger, the legal standard for “payment” arguably is met through clear and definitive evidence for direct exchange of the instrument, physical or virtual, representing legal tender. Accordingly, concepts of delivery and relinquishment of control fundamental to payment in cash have a clear analogy in the irrevocable transfer of digital banknotes through the FPN, and the fundamental legal principles underlying “payment” in cash should apply equally to payment in digital banknotes.

87 See Arthur Nussbaum, Legal History of American Currency 94 (1950) (“Because in monetary intercourse the recipient of money is chiefly concerned with its numerical relationship to the ideal unit, it is imperative that he be spared the necessity of inquiring into the title of the person who gives him the money.”); see also, e.g., Merchs. Loan & Trust Co. v. Lamson, 90 Ill. App. 18, 20 (Ill. App. Ct. 1899) (“even if money transferred to an honest taker was obtained by the one transferring it through a felony, yet the honest taker, who received it without knowledge of the felony and in due course of business, would acquire good title as against the one from whom it had been stolen.”) (citations omitted); Nassau Bank v. Nat’l Bank of Newburgh, 54 N.E. 66, 67 (N.Y. 1899) (“[W]hen money has been received by a person in good faith, in the usual course of business and for a valuable consideration, it cannot be pursued into his hands by one from whom it has been obtained through the fraud of a third person.”); Wyer v. Dorchester and Milton Bank, 65 Mass. (1 Cush.) 51, 53-54 (1853) (quoting and citing Miller v. Race (1758) 97 Eng. Rep. 398; 1 Burr. 452 (KB) (Mansfield, Lord C.J.)); Depew v. Robards, 17 Mo. 580, 582 (1853) (“At an early period of our commercial law, it was held, that money and bills payable to bearer, though stolen, could not be recovered after they had been passed away to a bona fide holder, and this by reason of the course of trade which creates a property in the holder. They pass by delivery only, and are considered as cash, and the possession of a bona fide holder always carries with it the property. This rule is founded on the necessity of sustaining the credit of that which is used as the medium of exchange in commercial transactions.”).
L.1.2, Addressing Gaps in the Legal Sources

The solution should identify any known gaps in legal sources with respect to the proposed legal Framework for the Solution and describe any plans to address those gaps.

L.1.2.1, Federal Reserve Act Amendments

As described above, there is a reasonable argument that the Fed has the authority to issue Federal Reserve notes pursuant to Section 16(1) of the Federal Reserve Act.\(^88\) Nonetheless, as also noted above, (i) digital banknotes did not exist at the time the statute was enacted and so there is a fundamental lack of clarity as to their coverage by the Federal Reserve Act and (ii) other paragraphs in Section 16 clearly contemplate printed notes, adding to the ambiguity as to the Fed’s authority in this regard. Moreover, other ambiguities exist. For example, the FPN requires electronic notes in all denominations (including fractional denominations) in order to satisfy the commercial test of serving as a true substitute for physical currency, both coin and paper. However, it is unclear whether Section 16(8) of the Federal Reserve Act, 12 U.S.C. § 418, authorizes issuance of notes in denominations less than one dollar. In addition, if the Fed determined to pursue a Bank Light model, a potential gap exists with respect to the Fed’s authority to establish a payment system reaching the public directly, i.e., a payment system through which a user could interact directly with the Fed to pay another remote user. Specifically, Paragraphs (1) and (14) of Section 16 appear to grant the Fed authority to issue and provide Federal Reserve notes solely to the Federal Reserve Banks. Recognizing the importance of these basic questions as to the Fed’s authority to issue digital banknotes, we propose below a potential amendment to the Federal Reserve Act that would address this and related issues. Although this Proposed Amendment is specifically designed to accommodate the proposed FPN, we have drafted with a technology-neutral approach to maintain the Fed’s flexibility under this proposed authority.

Proposed New Paragraph 18 to Section 16

18. **Digital Federal Reserve notes (Fed notes).**

   (A) The Board of Governors of the Federal Reserve System may issue Federal Reserve notes (Fed notes) in electronic form, including in electronic transferable records, subject to the requirements of this Paragraph 18. Federal Reserve notes issued pursuant to this Paragraph 18 are referred to below as “digital Federal Reserve notes.”

   (B) Except to the extent specified by Federal law enacted after the date of enactment of this Paragraph 18 or by regulation of the Board of Governors of the Federal Reserve System published after such date, all references to Federal Reserve notes in the Federal Reserve Act or other law or regulation shall be

---

\(^{88}\) We note that the FPN contemplates individual digital banknotes whose images viewed through an Internet browser “bear upon their faces a distinctive letter and serial number… assigned” by the Fed, consistent with Section 16(3) of the Federal Reserve Act. 12 U.S.C. § 413.
deemed to include digital Federal Reserve notes, which shall be currency of the United States.

(C) The Board of Governors of the Federal Reserve System may issue digital Federal Reserve notes only if it determines by regulation or order after notice, public comment and testing that its system for the issuance and distribution thereof is secure and can reliably and conclusively establish the record of ownership of such digital Federal Reserve notes and the transfer thereof.

(D) Ownership of and title to each digital Federal Reserve note shall be determined conclusively by the records of the Board of Governors of the Federal System. Transfer of such ownership and title shall be effected by recording of the transfer on the records of the Board of Governors of the Federal Reserve System. The recording of such a transfer by the Board of Governors of the Federal Reserve System shall constitute delivery of the associated digital Federal Reserve note.

(E) The Board of Governors of the Federal Reserve System shall promulgate from time to time regulations as it determines to be necessary or appropriate to give effect to the authority granted under this Paragraph 18, including with respect to:

(i) the format, distribution, mode of circulation, and mechanism for removal from circulation or destruction of such digital Federal Reserve notes;
(ii) the recording and publication of ownership of such digital Federal Reserve notes; and
(iii) the security of the systems used for such purposes.

(F) Digital Federal Reserve notes may be issued in any denomination set out in Paragraph 8 of this Section 16 and in any fraction thereof determined by the Board of Governors of the Federal Reserve System. References in this Section 16 to the physical printing of Federal Reserve notes shall be inapplicable to digital Federal Reserve notes.90

We note that the forgoing language attempts to establish the basic concepts of ownership, control, transfer and delivery of digital banknotes on the basis of the system of record controlled by the Fed pursuant to the Faster Payments Network, but does not attempt to further articulate the implications for all other principles of commercial law that would follow from this foundation. We believe that commercial law standards are better left to the development of

---

89 In the case of the FPN, the GDS would associate a specific digital Federal Reserve note (Fed note) with the specific public key issued to a specific, validated individual.
90 If the Fed determined to issue digital banknotes other than to the Federal Reserve banks for further distribution through financial institutions, additional modifications to the Federal Reserve Act would be necessary.
common law as they have for centuries, and that if further statutory changes become necessary at the state level, those can be pursued in the ordinary course. While there may be some temptation to take this opportunity to, in effect, establish a Federal commercial law on the basis of the underlying fiat virtual currency, we respectfully suggest that such an effort would jeopardize support for the creation of the currency itself.

Of course, the foregoing is only the preliminary draft of language to address a complex set of issues. If the Fed is supportive of the concept of digital banknotes, we would be pleased to work together to craft language that could be promoted in Congress.

**L.1.2.2, Other Gaps**

Other potential gaps to be considered are: (i) perfecting a security interest in digital banknotes, and (ii) levy and execution against digital banknotes.

**Perfection of a security interest in digital banknotes**

Security interests in personal property are governed by Article 9 of the Uniform Commercial Code (UCC) as enacted in the various states. Under Article 9, electronic currency, as legal tender, falls within the definition of “money”: “a medium of exchange authorized or adopted by a domestic or foreign government and includes a monetary unit of account established by an intergovernmental organization or by agreement between two or more nations.”[^91] This definition is inclusive of, and broader than, “legal tender.”[^92] Pursuant to the Proposed Amendment, digital banknotes would be included in the definition.

Under the UCC, “a security interest in money may be perfected only by the secured party’s taking possession under Section 9-313.”[^93] Section 9-313, “When Possession by or Delivery to Secured Party Perfects Security Interest Without Filing,” provides:

[A] secured party takes possession of collateral in the possession of a person other than the debtor, the secured party, or a lessee of the collateral when:

1. the person in possession authenticates a record acknowledging that it holds possession of the collateral for the secured party’s benefit; or
2. the person takes possession of the collateral after having authenticated a record acknowledging that it will hold possession of collateral for the secured party’s benefit.[^94]

In the case of the FPN, “control” of the digital banknotes is represented by possession/knowledge of the private key that permits the transmission of effective delivery instructions to the Fed.

[^91]: UCC § 1-201(24).
[^92]: See UCC § 1-201 cmt. 24. (“The test adopted is that of sanction of government, whether by authorization before issue or adoption afterward, which recognizes the circulating medium as a part of the official currency of that government. The narrow view that money is limited to legal tender is rejected.”).
[^93]: UCC § 9-312(b)(3).
[^94]: UCC § 9-313(c).
Levy and execution against digital banknotes

As a general matter, a judgment creditor has the right to enforce against money by serving a writ of execution on the appropriate legal officer, and directing him to levy against money in the judgment debtor’s possession or if it is identifiable as the judgment debtor’s money.95 However, state statutes on point generally contemplate levy against physical money — providing, for example, that “money, generally, may not be seized under execution when on the person of the debtor because such a taking would lead to breaches of the peace and physical conflicts and the violation of constitutional rights not permissible in the enforcement of civil process.”96 Similarly, a creditor generally has the right to levy by garnishment of a bank account; however, digital banknotes need not be held in a bank account. Finally, states provide for various types of levy against intangible property. 97

From a practical perspective, assuming a state’s statute allows for execution and levy against digital banknotes, the FPN’s architecture permits levy against banknotes held by an entity. The Fed will have the technical ability to refuse to honor transfer instructions directly, in its capacity as the custodian of the transfer record, and/or transfer the digital banknotes to the judgment creditor or its representative by issuing a new key pair to the party successfully executing garnishment or levy, in each case pursuant to appropriate judicial process — a process similar to garnishment of a bank account. In this regard, we would be pleased to cooperate with the Fed to review the technical aspects of the FPN that permit this functionality and determine agreeable regulatory language accommodating levy and execution.

L.1.3, Legal Obligations of Entities

The Solution should describe how entities and payments through the payment system (from Payer to Payee) will be legally bound within the proposed legal framework for the solution.

As indicated in L.1.1.4 on page 139, the Fed notes will be legal tender. Accordingly, the common law of tender and payment should apply to the rights and obligations of payees and payers using digital banknotes to the same extent as when making payment using physical currency. Obligations of financial institutions providing distribution services through a Bank Centric model would be required to agree to a Federal Reserve Operating Circular governing those processes. We note that the FPN’s architecture will provide holders of digital banknotes with several ways in which they may rely on financial institutions or other service providers to provide access to their private keys (or provide other functionality), with or without surrendering control of the key to the service provider. For example, the FPN accommodates an open standard for authentication of holders of digital banknotes by a service provider, enabling the holder to authorize the service provider to execute transactions using a username and password or other credentials, but without being required to entrust the key to the service provider. Alternatively,

96 Id. § 203.
97 See, e.g., Va. Code Ann. § 8.01-512.3 (2016); Int’l Fid. Ins. Co. v. Ashland Lumber Co., 463 S.E.2d 664, 666-67 (Va. 1995) (“The writ of fieri facias creates a lien in favor of the judgment creditor only to the extent that the judgment debtor has a possessory interest in the intangible property subject to the writ.”).
the FPN’s architecture supports the issuance of an additional private key to the service provider, the functionality of which may be limited, for example, to executing instructions validated by the holder of the digital banknote. We would be pleased to discuss these and other ways in which holders may rely on service providers to provide functionality related to digital banknote transactions, without surrendering control of the private key.

L.1.4, Compliance with U.S. Law

The Solution should describe how it supports compliance with relevant U.S. law by all end users and providers when sending and receiving payments. U.S. law includes OFAC, AML, BSA, the UIGEA (Regulation GG), Federal Consumer protection regulations (such as Regulation E and Regulation Z), Federal and State MSB laws, and all other applicable federal and state laws.

L.1.4.1, OFAC, AML and BSA Regulation

OFAC is an office of the Treasury responsible for enforcing sanctions against trade with designated persons and entities pursuant to various Executive Orders and statutes.98 AML regulations refer primarily to requirements imposed by the Bank Secrecy Act99 and the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 100

Together, OFAC, AML and BSA rules broadly require financial institutions (and other companies with respect to certain provisions) to refrain from transacting business with certain individuals and entities, to monitor certain financial activities for suspicious transactions, and to ensure that processes and procedures are in place to prevent prohibited acts. Transactions in physical cash are notoriously difficult to regulate for these purposes. However, the FPN offers a vast improvement over physical money.

First, under the Bank Centric model, digital banknotes would be distributed through financial institutions only to individuals whose identity has been validated in accordance with regulations that the Fed would promulgate pursuant to the Federal Reserve Act authority referenced above. Similarly, in order to be eligible to receive digital banknotes in the Bank Centric model, a person’s identity would need to be validated by an authorized financial institution before that person could receive a key pair enabling that person to transact in digital banknotes. Accordingly, subject to the appropriate regulatory provisions, both senders and recipients of digital banknotes could be vetted at the initial point of entry to the system for purposes of OFAC, AML and BSA. Under the Bank Light model, these functions would be performed directly by the Fed.

With respect to on-going OFAC monitoring, the Fed would need to determine its preference for reviewing previously issued keys when sanctions lists are updated. Under the Bank Light model,

99 31 U.S.C. §§ 5311 et. seq. (BSA)
the Fed would perform this function separately, since it would be the central repository of the relevant data. If the Fed sought to place this obligation on the financial institutions that originally validated customer identity, the Fed would need to consider the cost impact to financial institutions of such a burden, since the institutions would not necessarily have on-going relationships with the persons whom they set up in the system in the first instance. In either case, only the Fed would be in the position to block transfers in compliance with applicable sanctions regimes, and therefore would require a system to receive notice of blocked digital banknotes.

Furthermore, because digital banknotes need not be held in accounts, financial institutions involved in the initial distribution of digital banknotes to users would not necessarily be in the position to monitor on-going transactions. However, since the Fed would be the central repository of information regarding all transactions in digital banknotes, the Fed will be in a position to undertake, or enable other agencies to undertake, unprecedented real-time monitoring of the flow of funds in the digital banknote system. With strong front-end identity verification requirements, the FPN would enable AML-related controls far exceeding those currently in place for cash transactions. In addition, as alluded to above, the FPN architecture supports a multi-tiered approach to the user base, with holders who have not undergone bank identity verification subject to hard-wired transactional limits (e.g., based on the number or dollar value of transactions during a specified period), while holders who have undergone screening may be subject to less stringent limits, or, if the digital banknotes held by such users are linked to an account, no limits other than restrictions applicable to those of any other holder of a bank account (e.g., standard OFAC blocks and suspicious activity reporting). Such a multi-tiered approach would both preserve widespread access to digital banknotes, and allow financial institutions to maintain their gatekeeper role for transactions at levels designated by the Fed. If the Fed is supportive of the FPN, we would be pleased to consult with the Fed and the relevant stakeholders to determine a prudent approach.

**L.1.4.2, Regulation E and UCC Article 4A**

Regulation E, promulgated pursuant to the Electronic Funds Transfer Act, “applies to any electronic fund transfer that authorizes a financial institution to debit or credit a consumer’s account.”\(^{101}\) An “electronic fund transfer” means “any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account.”\(^{102}\) With respect to the transfer of digital banknotes directly between end users, Regulation E therefore would be inapplicable since no “account” would be involved. Indeed, the framework on which the FPN is based, functional equivalence to cash, is fundamentally inconsistent with the Regulation E error resolution regime. The FPN does not contemplate the Fed providing an error resolution framework. Instead, as with payments in physical currency, transactions through the FPN are final and irrevocable. Claims related to mistake, theft, etc. must be made outside the FPN through other legal avenues. For this reason, the Fed may wish to undertake a consumer

---

\(^{101}\) 12 C.F.R. § 205.3(a) (2016).

\(^{102}\) Id. § 205.3(b).
education campaign in connection with the launch of digital banknotes to ensure consumer awareness of this feature of the FPN.\textsuperscript{103}

UCC Article 4A governs certain credit transfers over large-value networks as well as ACH. “Funds transfers” for purposes of Article 4A are triggered by a “payment order” from the sender of funds, “made for the purpose of making payment to the beneficiary of the order.”\textsuperscript{104} “A funds transfer is completed by acceptance by the beneficiary’s bank of a payment order for the benefit of the beneficiary of the originator’s payment order.”\textsuperscript{105} “Payment order’ means an instruction of a sender to a receiving bank to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary” if, among other conditions, “the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender” and “the instruction is transmitted by the sender directly to the receiving bank or to an agent, funds-transfer system, or communication system for transmittal to the receiving bank.”\textsuperscript{106}

Accordingly, a “payment order” issued to a “bank” to pay a beneficiary — whether the payment is in digital banknotes, physical notes, or electronic funds — is covered by Article 4A. The Federal Reserve Banks are “banks” for this purpose. However, it is unlikely that the Fed in its capacity as controller and, potentially, operator of the Internet domain representing digital banknotes would be considered a “bank” for purposes of the statute. “Bank” means “a person engaged in the business of banking and includes a savings bank, savings and loan association, credit union, and trust company. A branch or separate office of a bank is a separate bank for purposes of this proposal.”\textsuperscript{107} We do not believe that the Fed, in its capacity as the issuer of fiat currency is engaged in the business of banking. It would not be taking deposits, making loans or performing any of the other functions associated with a banking business; rather it would be engaged in the sovereign operation of distribution and maintenance of the money supply. For these reasons, Article 4A does not, by its terms, apply to the Fed’s role in the issuance of digital banknotes.

However, we note here that the inapplicability of Regulation E and UCC Article 4A may change in the Bank Centric model. If, for example, banks play an on-going intermediary role by housing private keys, or act as distributors and depositories of digital banknotes, Regulation E and Article 4A may govern their activities.

We also note that, notwithstanding the applicability of Regulation E and Article 4A, various states and the Consumer Financial Protection Bureau have expressed concern with respect to the adequacy of consumer disclosures in connection with non-fiat virtual currencies. These concerns center on finality of transactions, security and value fluctuation. As explained above, the concept of finality of payment under the FPN is consistent with the treatment of transactions in physical

\textsuperscript{103} The Consumer Financial Protection Bureau (CFPB) has expressed an ongoing interest in consumer awareness of virtual currency and the role of virtual “wallets” in the Regulation E context. We feel that a consumer information campaign regarding the FPN could be folded into the CFPB’s outreach efforts with respect to virtual currencies.

\textsuperscript{104} UCC § 4A-104(a).

\textsuperscript{105} Id.

\textsuperscript{106} Id. § 4A-103(a).

\textsuperscript{107} Id. § 4A-105(a)(2).
currency rather than with the unauthorized use and error resolution standards in Regulation E. Accordingly, we would propose crafting disclosures for public consumption that highlight the finality of digital banknote transactions. Similarly, like transaction finality, security risks should be treated as a disclosure matter under the FPN. The Fed will adopt the solution only if it is satisfied with the underlying security of the PKI that supports the issuance and transfer of digital banknotes. Real security issues, therefore, relate not to the core technology, but to the means by which end users maintain and secure the private keys used to interact with the FPN. As with any other technology, the market will continue to evolve with respect to security features that might be layered into software and hardware to help prevent unauthorized access to and use of an end user’s private keys. While the Fed may attempt to set some standards in this regard, end users ultimately must be advised that they are responsible for the protection of their private keys. Finally, value fluctuation concerns are not at issue under the FPN because the digital banknotes will have a fixed denomination and value specified by the Fed as a fiat currency no different than physical banknotes.

L.1.4.3, Regulation Z

The FPN does not contemplate the extension of credit, or otherwise come within the scope of Regulation Z. Accordingly, it is inapplicable to the FPN.

L.1.4.4, Uniform Money Services Act (UMSA) and similar statutes governing money services

The UMSA, promulgated by the National Conference of Commissioners on Uniform State Laws in 2000 and amended in 2004, provides that a person may not engage in specific regulated activities (money transmission, check cashing, and currency exchange) unless they hold a qualifying license or are an authorized delegate of a person holding a qualifying license. The Fed does not require a license under the UMSA (or any other similar state law) to issue digital banknotes. Furthermore, bank distributors of digital banknotes would be exempt from the UMSA. UMSA § 103(4). Similar exemptions exist in states that have not adopted the UMSA. See, e.g., N.Y. Banking Law § 641(a) (McKinney 2016).

Whether regulated non-bank providers might be deemed to be engaged in money transmission will depend on the activities in which they engage in connection with digital banknotes. Since digital banknotes will constitute “money,” a regulated non-bank provider that takes control of an end user’s private key for purposes of facilitating transfers by the end user may be considered to be engaged in “money transmission.”

108 12 C.F.R. §§ 226.1 et seq.
109 See UMSA §§ 201(a), 301(a), 401(a).
110 The Fed is also exempt on the face of the UMSA. See UMSA § 103(1) (exempting “the United States or a department, agency, or instrumentality thereof”).
111 See UMSA § 102(14).
112 It should be noted in this regard that the Uniform Law Commission is in the process of drafting a Regulation of Virtual Currency Business Act. As currently constituted, however, that Act would not apply since its definition of “virtual currency” excludes “money.”
L.1.4.5, Privacy laws between holders of digital banknotes and providers of wallets or other functionality

The Gramm-Leach-Bliley Act (GLBA)\textsuperscript{113} places certain limitations on disclosure of non-public personal information by financial institutions, i.e., banks and other companies whose activities are financial in nature.\textsuperscript{114} Such companies also must ensure the security of customer personal data, and maintain policies to ensure such security.\textsuperscript{115} The Federal Trade Commission (“FTC”) has interpreted “financial company” broadly to include, for example, automobile dealerships, businesses that print checks, tax preparers, and other entities far beyond banks that may come routinely into contact with consumer financial information.\textsuperscript{116} Given the breadth of this definition, it is likely that a third party that houses credentials, including private keys, for users of digital banknotes, would be determined by the FTC to be within the scope of the GLBA. The FPN would not require disclosure of consumer financial information in a manner that would otherwise be restricted by the GLBA. The FPN will allow holders of digital banknotes to give permission to make their record ownership public, thus enabling holders to possess digital banknotes and execute transactions in a way that is visible to the public, if they so choose. Privacy concerns are thus easily addressed by express “opt-in” consents in circumstances where public knowledge of digital banknote ownership would serve a specific public policy. In any event, the system may be configured to enable the Fed to require privacy (or publication) of certain transfers, if desired.\textsuperscript{117}

Unlawful Internet Gambling Enforcement Act

The Unlawful Internet Gambling Enforcement Act\textsuperscript{118} (UIGEA) provides that “[n]o person engaged in the business of betting or wagering may knowingly accept, in connection with the participation of another person in unlawful Internet gambling[.], (1) credit . . .; (2) an electronic fund transfer . . .; (3) any check, draft, or similar instrument; or (4) the proceeds of any other form of financial transaction” as may be determined by regulation, in each case “on behalf of such other person.”\textsuperscript{119} UIGEA directs the Secretary and Federal Reserve to prescribe regulations “requiring each designated payment system to identify and block restricted transactions.”\textsuperscript{120} A designated payment system is defined as “any system utilized by a financial transaction provider that the Secretary [of Treasury] and the Board of Governors of the Federal Reserve System jointly determine could be utilized in connection with, or to facilitate, any restricted transaction.”\textsuperscript{121} The Fed and the Secretary of the Treasury have designated five payment systems: ACH systems, card systems, check collection systems, money transmitting businesses, and

\textsuperscript{115} See 16 C.F.R. § 314.4 (2016).
\textsuperscript{116} See id. § 313.3(k)(2).
\textsuperscript{117} We note that, whether a transaction record is public or private, holders of digital banknotes will retain the ability to authenticate ownership using their private keys.
\textsuperscript{118} 31 U.S.C. § 5361 et. seq.
\textsuperscript{119} Id. § 5363(1)–(4).
\textsuperscript{120} Id. §5364(a).
\textsuperscript{121} Id. §5362(3).
and wire transfer systems. However, participants in some of these systems are exempt from application of the UIGEA, except for institutions who have a relationship with the recipient of funds, i.e., the institution that engages in gambling activity.

As indicated above in connection with the discussion of OFAC, AML and BSA, the party engaged in the initial verification of identity of a person authorized to transact in digital banknotes (financial institutions in the Bank Centric model or the Fed in the Bank Light model) would have the opportunity to perform initial diligence on whether a prospective end user is an unlawful Internet gambling business. However, that party may not be in the position to monitor transactions by an approved end user on an on-going basis, while the Fed will have access to a large pool of centralized data. Accordingly, as in the case of OFAC, AML and BSA, the Fed will need to consider adopting regulations and/or a governmental monitoring regime to satisfy the goals of UIGEA.

Laws Against Counterfeiting

By their terms, laws against counterfeiting currency would apply to digital banknotes as obligations of the United States to the same extent as physical Federal Reserve notes. See, e.g., 18 U.S.C. §§ 470–473.

L.1.5, Unique Legal Provisions

The Solution should identify any unique legal provisions needed in the Solution’s legal framework to address any situations in which end users and providers will perform the same functions in the payment system, but are subject to different applicable U.S. banking and payment laws and/or regulatory supervision.

The law governing the basic commercial elements of payment should not vary depending upon the counterparty that any end user may face in a payment using digital banknotes. While providers may be subject to different licensing regimes depending on their charters and roles in the handling of digital banknotes, no unique legal provisions are necessary since the treatment of digital banknotes as “money” will effectively enable the FPN to rely on existing legal standards in that regard.

L.2, Payment System Rules

Payment system rules means that the solution should have requirements, standards/protocols, and procedures that govern the rights and obligations of all end users, providers, Payers and Payees.

\[122\) See 12 C.F.R. § 233.3.
\[123\) See id. § 233.4; Prohibition on Funding of Unlawful Internet Gambling, 72 Fed. Reg. 56,680, 56,685 (Oct. 4, 2007) (“The Agencies are proposing to exempt all participants in the ACH systems, check collection systems, and wire transfer systems, except for the participant that possesses the customer relationship with the Internet gambling business.”).
L.2.1, Inclusion of Key Features

The Solution should describe key features of existing or proposed payment system rules governing the rights and obligations of all end users, providers, Payers and Payees to enable the payment system to operate effectively and efficiently, including payment system rules addressing the following areas, which are detailed in this document:

- Authentication of all entities, payments or messages connected to a payment
- Legal responsibility of providers that provide payment system access to end users
- Payment order initiation/authorization and termination of authorization
- Cancellation of a payment
- Delayed and failed payments
- Payment finality and settlement
- Timing of sending and receipt of a payment
- Records as proof of payment for Payers and Payees
- Error resolution for most anticipated disputed payments among end users, providers, Payers and Payees

L.2.1.1 Authentication of all entities, payments or messages connected to a payment

The FPN’s rules require authentication (see S.2, S.5.4, S.5.5, S.7.1, S.10) by all entities participating in the payment system. The payment system allows individuals to establish their authentication credentials (e.g., username and password) and optional supported multifactor credential. The FPN also allows devices to authenticate to the system; however, device connections and permissions are granted, managed and controlled by the end user to whose payment address the device connects.

L.2.1.2 Legal responsibility of Providers that provide Payment System access to end users

Providers have legal responsibilities related to their roles as participants in the payment system. Depository institutions, in addition to their roles as participants, have legal roles and responsibilities as distributors of Fed notes. It is proposed that the payment system is governed by the Governing Organization and centrally controlled by the Federal Reserve.

L.2.1.3 Payment order initiation/authorization and termination of authorization

A payment order consists of at least three items of information: the source payment address (the Payer or holder of the Fed notes), the destination payment address (the Payee), and the transfer amount. The FPN permits only the Payer, the holder of Fed notes, to sign and submit a payment order to the system. Before a payment order can be submitted by the Payer, s/he must authenticate to the system (see S.10.1). After successful authentication, the Payer is permitted to complete a payment order by selecting a Payee's payment address and entering the amount to send. The Payer can cancel or terminate the payment order by selecting cancel on the system.

---

124 Multifactor authentication may be required depending on the role of the individual (see S.5.4) and total value that may be held in the payment address (see S.10.4).
dialog. If the Payer chooses to fill in the amount on the dialog and clicks send, s/he has authorized, signed and submitted the payment order to the system.

The payment system rules indicate that when the Payer fills out the payment order, signs it, and submits it for execution, the payment system will execute the Payer’s instructions as submitted and attempt to complete the transfer. If the Payee has not activated payment codes, then the system will display either an error or a confirmation to the Payer. The transfer is final when the payment system displays the transfer confirmation page. If the Payee has activated payment codes, then the payment system displays the payment code page with options for the Payer including an option to cancel the code.

If the Payer is not in possession of Fed notes, then the payment system option allowing the Payer to select a destination address is disabled. Only when the Payer holds transferable value will the payment system display the payment order dialog (aka “send dialog”) to the Payer. The FPN’s technical design has no provisions for overdraft.

The Payer may cancel payment orders prior to submission for processing. The Payer may also terminate or cancel a payment code or pre-authorization at any time before it has been accepted by the Payee. The Payer’s cancellation of a payment code works like the cancellation of a preauthorized payment.

L.2.1.4 Cancellation of a Payment

The FPN’s rules permit the cancellation (or retraction) of transfers under any of the following conditions:

- The transfer is preauthorized and Payee has not received or validated the payment code that was uniquely generated by the payment system.
- The transfer is in an “invitation” status, and the transfer has not yet been accepted by the recipient.
- A signed payment order has not been submitted to the system.

The FPN’s rules do not permit cancellation or revocation of a signed payment order that was submitted by the Payee to the payment system.

L.2.1.5 Delayed and Failed Payments

The FPN executes the Payer’s signed and submitted payment orders with no delay and without human intervention. When a payment order has completed successfully, the payment system displays a payment confirmation page\(^\text{125}\) where the Payer can view the completed transfer along with other contextual information. If the payment system is not able to complete the payment

\(^{125}\) Confirmation information is displayed in the context of the application that is being used by the Payer to submit the payment order; consequently, confirmation information may be displayed in a dialog or some other manner rather than a web page.
order (i.e., a failed payment), the payment system displays an appropriate error message to the Payer, and the failed payment is recorded by the system.

L.2.1.6 Payment Finality and Settlement

The FPN’s rules require that payment orders that include the transfer of Fed notes are final (see S.3) and irrevocable. Because Fed notes are transferred without delay, settlement is completed concurrently with the execution of the payment order, eliminating credit and liquidity risks or exposures associated with a possible lag in time between funds availability and final settlement (see S.4.2, F.4.1, E.5.1).

L.2.1.7 Timing of sending and receipt of a payment

The FPN executes signed payment orders upon submission by Payer and displays a confirmation page to the Payer when payment is successful. The payment system also notifies both the Payer and Payee that the transfer is complete using the primary communication channel (e.g., email or SMS/text) and, if applicable, alternate communication channels (e.g., in-app notification on smartphone, tablet or desktop computer). The Payee receives good funds immediately when execution of the Payer’s payment order is completed by the system.

L.2.1.8 Records as Proof of Payment for Payers and Payees

The FPN keeps a record of all executed payment orders and makes this information available to both the Payer and the Payee. Records are retained according to regulatory requirements (see U.4, E.7).

L.2.1.9 Error Resolution

This section details error resolution for most anticipated disputed payments (see S.5) among end users, providers, Payers and Payees.

The FPN’s rules require that the Payer authenticate to the payment system using valid credentials to sign and submit payment orders for the transfer of Fed notes. The payment system rules allow only the Payer and not the Payee to submit payment orders for the transfer of Fed notes. The Payer is required to agree to waive rights to have disputes mediated through the Federal Reserve, the Governing Organization, the Payer’s depository institution or regulated non-bank provider, or another stakeholder in the transfer each time the Payer signs and submits a payment order to the payment system.

The FPN’s rules hold the Payer accountable and financially responsible for errors in signed payment orders submitted by the Payer and executed by the payment system. The rules hold the Governing Organization accountable and financially responsible for systemic breaches that cause loss to Participants.

L.2.2, Development of and Amendment to Rules

If different from the process set forth in G.1 and G.2, the Solution should describe the process that was or will be used for the development and amendment of the payment system rules, including the process for obtaining input from payment system stakeholders.

The FPN’s process that will be used for the development and amendment of payment system rules is set forth in G.1 on page 160 and G.2 on page 162.
L.2.3, Enforcement and Monitoring of Rules

If different than the process set forth in G.1 and G.2, the Solution should describe how payment system rules will be enforced and monitored, including whether or not an organization or regulators may enforce the rules.

The FPN’s description for how payment system rules will be enforced and monitored are set forth in G.1 on page 160 and G.2 on page 162. The rules permit the Governing Organization and the Federal Reserve as the regulator to enforce the rules.

L.2.4, Allocating Responsibility for Authorization

The Solution should describe existing or proposed payment system rules for allocating legal responsibility to appropriate entities to obtain valid authorization from the Payer.

The FPN’s rules allocate legal responsibility to all participants through participation agreements for each applicable party including the following:

- Individuals or natural persons,
- Businesses, including federal, state and local governments
- Depository institutions with responsibility to distribute Fed notes

The FPN’s rules permit only the Payer using valid credentials and acting on its own behalf to sign and submit a payment order to the payment system. The FPN’s technical design does allow a person to safely authorize another person to complete, sign and submit payment orders on her behalf without sharing credentials. The authorization to submit a payment order on behalf of another must be specifically granted by the Payer from whose payment address the funds originate.

For example, the FPN’s technical design allows John to grant permission to Linda to proxy John’s payment address. After proxy permission is granted by John to Linda, Linda can proxy John’s payment address using her own credentials and complete, sign and submit payment orders for John. Because John granted Linda proxy permission, the funds originate from John. However, the payment order is still signed by Linda using her credentials. John doesn’t share his credentials with Linda. John can also revoke Linda’s proxy permission at any time.

L.2.5, Error Resolution

The Solution should describe existing or proposed payment system rules related to an error resolution process within the payment system for end users and Providers to correct or otherwise resolve errors, unauthorized transactions or disputes in the payment process (see also S.5 and L.3).

The FPN’s rules hold the Payer accountable and financially responsible for errors in signed payment orders submitted by the Payer and executed by the payment system. The Governing Organization has responsibility to resolve system errors. Neither the Governing Organization nor the Federal Reserve as the issuer of Fed notes are responsible to arbitrate on behalf of the Payer or Payee in a payment dispute.
### L.3, Consumer Protections

Consumer protections means that the Solution should have a legal framework and procedures that allocate legal responsibility, allocate financial responsibility and support error resolution for payments made to or from natural persons for personal, family, or household purposes (see also S.5).

#### L.3.1, Allocating Responsibility for Losses

The Solution should describe a legal framework for allocating legal and financial responsibility for all entities for losses in the event of a Payer or Payee claim of unauthorized, fraudulent or erroneous consumer payments.

The FPN’s legal frameworks seeks to hold the Payer accountable and financially responsible for errors on signed payment orders submitted by the Payer and executed by the payment system. The Governing Organization is accountable and financially responsible for system errors in the payment system. The FPN’s rules do not permit the Payee to sign and submit a payment order on behalf of the Payer. The FPN is designed with protections to expressly prohibit and prevent the Payee from signing and submitting a payment order on behalf of the Payer. The FPN’s careful design and protections are intended to explicitly eliminate the Payer’s claims for unauthorized consumer payments. The Governing Organization and the Federal Reserve are not accountable nor financially responsible for errors on the Payer’s signed and submitted payment orders.

#### L.3.2, Rules for Error Resolution

The Solution should establish payment system rules and procedures that support error resolution for consumer claims arising from payments fraud, unauthorized payments or errors.

The FPN’s design, payment system rules and procedures seek to hold the Payer accountable and financially responsible for errors on signed and submitted payment orders executed by the payment system. The Governing Organization will be accountable and financially responsible for systematic errors. The FPN is carefully designed and engineered with protections, such as multi-factor authentication, push-only transfers, etc., to prohibit and prevent Payees from submitting payment orders on behalf of the Payer (i.e., unauthorized payments). The FNP is carefully designed to address first-, second-, and third-party fraud (see S.1.4).

#### L.3.3, Additional Consumer Protections

The Solution should include options for end users, Providers and the payment system to establish additional consumer protections for payments, which may exceed those protections that are otherwise required under applicable law.

The Governing Organization, with the supporting vote of its members that represent the various participant segments (e.g., financial institutions, business, consumers, governments, etc.), is authorized to establish or modify rules that may exceed those protections for end users and Providers that are otherwise required under applicable law.
**L.4, Data Privacy**

Data privacy means that the Solution should have 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. The Solution should also have an approach, consistent with law, to secure information that should not be disclosed (see also S.9).

**L.4.1, Approach to Privacy and Confidentiality**

The Solution should describe its approach to data privacy and confidentiality of payment and related data. For example, the legal framework should describe limitations on end users’ or Providers’ collection of data and use or disclosure of payment data to third parties.

The Governing Organization will establish and adhere to a privacy policy for the payment system that discloses the following to the end users and providers:

- What information the payment system collects
- How collected information is used
- What, if any, collected information is sold
- What control the participant has over collected information
- Collected information that can be removed and how to remove it
- How collected information can be updated
- How information collected is protected
- What collected information is shared
- Other important and relevant disclosures as may be included by the Governing Organization or required by rules, regulation or law

The policy also needs to be drafted to support end user’s sharing of information on social media sites including a customized payment address, payment address profile information and certain information related to transfers.

The Governing Organization will also be required to maintain and periodically update the privacy policy. End users should be informed when the policy is updated and be able to see easily what has changed and review prior versions of the privacy policy.

**L.4.2, Protecting Payment Data**

The Solution should describe its approach to data security of payment and related data, taking into consideration the application of legal requirements. For example, the legal framework should describe operational procedures and policies to secure data within the payment system and at end-user and provider locations.

The FPN’s comprehensive data security includes the following measures:

- The FPN implements and adheres to current and applicable Federal Information Processing Standards (FIPS).
- The FPN implements and adheres to applicable recommendations found in NIST Special Publications documents (e.g., NIST Special Publication 800-53 revision 4, Security and Privacy Controls for Federal Information Systems).
- The payment system, while available to the public at an Internet domain, has contextual data security for payment instruments (i.e., Fed notes), payment addresses, and payment address
aliases that may point to sensitive information (e.g., checking accounts). The payment instruments, payment addresses, and payment address aliases can only be accessed through the authorized domain. For example, a payment address alias that is a URL that points to a checking account is public and can be stored anywhere, but merely having the URL is insufficient to access the checking account; an end user must be authenticated and use the URL in the proper context for it to have functional value in the system.

- The collection of payment and related data is centralized, which limits the area of concern for the protection of sensitive data.
- End users and providers can access payment and related data only after authentication using credentials and under a participation agreement that includes requirements for protection of any downloaded copies of payments and related data.
- End users and providers access to payment and related data is limited to (a) public information, (b) sensitive information (such as a checking account) that is verifiably under their control, and (c) information about transfers where the end user or provider is a party to the transfer.

**L.4.3, End User Data Required**

The Solution should describe the nature and type of end-user data that may be required for security, legal compliance and authentication purposes within the solution.

**L.4.3.1, End User Data Required for Legal Compliance**

The FPN operates in accordance with regulations and laws including Anti-Money Laundering Compliance, Bank Secrecy Act, USA Patriot Act, OFAC, and other applicable laws and regulations. To comply with payment system rules, regulations, and laws, the Governing Organization may be required to collect, record and verify the following types of information for individual end users: the individual’s name, date of birth, address and qualifying identification number\(^{126}\) to show that the Governing Organization has a true identity of the end users. If the end user is a business, the Governing Organization may be required to collect, record and verify the following types of information: ownership information, articles of incorporation (or similar documents depending on entity type), business description, address, telephone number, financial statements, and banking references.

**L.4.3.2, End User Data Required for Security & Authentication**

The FPN’s technical design allows for end users to authenticate with only a credential, meaning that if an end user is using a hardware token that provides strong asymmetric digital signatures or an external identity service provider, the end user may, if permitted by the rules, establish and control a payment address using only the credential (see S.2 and S.10), omitting username and password.

\(^{126}\) FFIEC online manual.
L.4.4, Disclosure of Collected Data

The Solution should describe how end users may get visibility into the data being collected about them, limit sharing of such data, and change their privacy preferences with regard to proposed uses of end user data.

The FPN enables end users complete visibility and reasonable control over the data being provided by them or being collected about them by allowing the end user to authenticate to the payment system and view and/or update the following information:

- Complete transfer history for all transfers and each transfer’s associated contextual data.
- Profile information, including the end user’s optional custom (vanity) URL, profiles on social media sites (optionally linked by the end user to the end user’s payment address), and the written description about the end user.
- Optional contact information provided by the end user, including the end user’s phone number, website address, and home address.
- Other information related to the end user’s payment address, including businesses the end user manages and confirmed deposit accounts held with depository institutions and regulated non-bank providers.

L.4.5, Data Breaches

The Solution should describe its approach to data breaches at the payment system or at an end user/Provider, the responsibilities (including notifications) of the end users/providers in the event of such a breach, and whether the legal framework seeks to allocate financial or other responsibility among end users and providers in the event of a data breach.

The FPN’s data is stored centrally. The Governing Organization is responsible to protect and ensure security of the payment system against data breaches and threats. The Governing Organization is accountable and financially liable for security and data breaches except where the end users are responsible to protect and secure information. In the event that the Governing Organization’s liability for a breach exceeds its financial ability to pay, the Federal Reserve as the issuer and regulator will be the next financially liable party.

End users, including providers, are required to use strong passwords and are encouraged to choose an optional two-factor authentication method. End users are responsible to protect and secure their credentials. End users are accountable and financially responsible for a loss associated with the misuse or theft of their credentials.

L.5, Intellectual Property

Intellectual property means that the Solution should have an approach to address any risks arising from third-party rights related to patents, trademarks, copyrights, and trade secrets.
L.5.1, Managing Intellectual Property Risks

The Solution should set forth a proposed approach for the payment system, end users and providers to resolve or manage, prior to implementation, any legal, operational or financial risks arising from third-party intellectual property rights (including patents, trademarks, copyrights and trade secrets). The proposed approach should include whether or not the solution has undertaken or will undertake a due diligence review of potentially applicable intellectual property rights.

The FPN has been in operation since December 2010. It is operated by WingCash, LLC (the Company) a Utah Limited Liability Company founded on November 2, 2009, by W. Bradley Wilkes. The Company has a licensee to three patents granted by the United States Patent and Trademark Office (USPTO) related to the FPN as presented in this solution proposal. The three patent grants name W. Bradley Wilkes as the inventor and are patents 8,306,910; 8,630,951; and 8,706,626. The Company offers an open source version of the current embodiment of the FPN available at wingcash.org. The open source version is distributed under the GNU AFFERO GENERAL PUBLIC LICENSE, Version 3 (AGPL-3.0).

In January 2011, the inventor also conducted an international patent search through an international search authority under the Patent Cooperation Treaty (PCT) for the claims found in application patent grant #8,630,951. The written opinion of the international searching authority found claims 1-25 to be novel and inventive and to have industrial applicability. The inventor did not seek to nationalize the international application with other national or regional authorities under the PCT. The holder of the patents is willing to license or transfer the patents to the Federal Reserve or the Governing Organization under mutually acceptable terms.

The FPN’s open source application stack (e.g., PostgreSQL, RabbitMQ, Python, Pyramid, SQLAlchemy, Memcached, Buildout, Twisted, Ionic) can be replaced with equivalent proprietary applications from other vendors (e.g., IBM) to achieve faster payment capabilities of the proposed solution.

Part C, Section 6: Governance

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>Section &amp; Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Governance</td>
<td>G.1, Effective Governance</td>
<td>✔️</td>
</tr>
<tr>
<td>Governance</td>
<td>G.2, Inclusive Governance</td>
<td>✔️</td>
</tr>
</tbody>
</table>

G.1, Effective Governance

Effective governance means that the Solution should have decision- and rule-making processes that are transparent and support both the Solution’s objectives and public policy objectives.
G.1.1, Efficiency

The Solution’s governance arrangements (e.g., policies and structure) should ensure efficient decision-making and rule-making, including establishing clear lines of responsibility for all decision makers or decision-making bodies.

The FPN’s authors suggests that operating and governing roles and responsibilities be divided among the following entities (the parties):

- The Federal Reserve
- A chartered Governing Organization (the Governing Organization)
- Various other independent entities that will provide certain governance functions (see G.1.4) on a contractual basis

The governance arrangements and division of responsibilities will be thoroughly documented, agreed to by all parties, and appropriately communicated to the public (see G.1.2).

The Governing Organization is proposed to be a not-for-profit, membership-based organization whose responsibilities include certain operations and administrative tasks different from tasks performed by the Federal Reserve and shared responsibility for rulemaking, compliance (see L.1.4), government relations, industry relations, community relations, and platform support. The Governing Organization will have sole responsibility for the following:

- Drafting and maintaining a certification program for integrators desiring to publish an application to the public.
- Conducting rigorous application tests to ensure that applications are performing according to published integration standards.
- Releasing and revoking integrator or application access to the platform.

The Governing Organization may also assist other entities in education and training for the system, events, tool development, innovation, closed-loop network design and administration, and closed-loop value distribution.

The Governing Organization will establish an independent board with diverse representation that is nominated and voted upon by the diverse membership of the organization. The members of the board will have fiduciary duty to the organization. The members of the board will have appropriate term limits and will approve the hire of the Governing Organization’s senior executives. The members of the board will not have voting rights for rules changes.

The Governing Organization will also establish various committees and advisory boards to assist with decision making. The committees and advisory boards will be composed of diverse interests and viewpoints to represent the various classes of participants in the platform (e.g., financial institutions of various sizes, businesses including large government users and retailers, small- and medium-sized business, regulators, etc).

The rulemaking process will allow proposed rule changes from any individual member, business or corporate member, or affiliate member or partner. Proposed rule changes will be published in a request for comment (RFC) to the members of the Governing Organization and the public at large. Unless otherwise indicated by the rulemaking process, it is expected that adopted RFC’s will be prioritized for implementation into the code of the system.
G.1.2, Public Disclosure

The Solution’s governance arrangements should be publicly disclosed.

The Governing Organization has the responsibility to update, maintain, and publish information relating to the governance arrangements between the Governing Organization and other Parties. The Governing Organization will publish governance arrangements on a website maintained by the Governing Organization. The Governing Organization may also determine other appropriate communication channels to publish governance arrangements.

G.1.3, Appeals Process

The Solution’s governance arrangements should provide a process to handle appeals related to specific decisions or their implementation.

The Governing Organization will establish and maintain processes to handle appeals related to specific decisions and their implementation. First, the Governing Organization will establish a decision-making framework to reduce the potential for appeals to specific decisions and their implementation. Second, the decision-making framework will require a consensus vote before decisions can be finalized and implemented. Finally, the decision-making framework will detail the process and timeframes for submission of an appeal to a decision prior to the implementation of the decision. The decision-making framework will be published and available for review by all members participating in the decision-making process and the full participating community.

G.1.4, Validation of Compliance

The Solution’s governance arrangements should provide for independent validation of compliance with the solution’s rules, compliance with applicable law, and achievement of both the solution’s objectives and public policy objectives.

The FPN’s authors recommend that the Governing Organization will hire independent reviewers to conduct regular and thorough code reviews to ensure that the FPN is operating according to rules, applicable law, and public policy objectives. The independent reviews will be comprehensive and will require the reviewer to conduct code reviews, security reviews, regulatory reviews and independent tests of the Governing Organization, the FPN, and its operations. For example, the reviewer may test an individual wallet approved for certain monthly transfer limits. Another example of an independent test may be for the reviewer to confirm that basic limits based on where the payment address owner is domiciled are correctly applied.

The FPN’s policy objectives are to enable the fast, efficient, and secure end-to-end payment capability for all American consumers and businesses. Achievement of the FPN’s policy objectives will be first demonstrated through consumer and business adoption and use.

G.2, Inclusive Governance

Inclusive governance means the Solution should allow for input and representation from diverse stakeholders (e.g., end users, operators, providers, and regulators) and support the public interest.

G.2.1, Public Interest

The Solution’s governance arrangements should include consideration of the public interest when making decisions and rules.
The Governing Organization’s processes for implementing new and changing rules will be as follows:

1. The membership of rule-making committees will be composed of a diverse group of individuals with differing opinions and perspectives that are representative of the diverse classes of participants using the platform.
2. Before rule changes can be adopted, the public will be allowed to comment on proposed rules changes, and the rule-making committee will be required to demonstrate that all comments from the public are addressed.
3. The rule making committee will also be required to publish how public comment was addressed in the rulemaking process.

G.2.2, Stakeholder Input

The Solution’s governance arrangements should provide for input and influence by all stakeholders through one or more governance or advisory bodies.

The Governing Organization will be required to define and establish voluntary advisory groups to allow stakeholders to influence the decision-making and rule-making processes. For example, the Governing Organization may establish a board advisory group, a government relations advisory group, a consumers advisory group, a large financial institutions advisory group, a medium financial institutions advisory group, and a small financial institutions advisory group. The advisory groups will have a voice and vote in the decision-making process, rule-making process, and other processes as appropriate.

G.2.3, Fair Representation

The Solution should have governance and advisory bodies that fairly represent stakeholders’ interests and risks.

The Governing Organization will create advisory bodies based on roles and responsibilities in the platform. For example, an advisory body can be created that is composed of various sizes of financial institutions. Financial institutions have the unique role and responsibility to be distributors of digital Fed notes. Because of the unique role depository institutions play as distributors, the Governing Organization will form an advisory group to represent the views, perspectives and interests of this important stakeholder group. The Federal Reserve, like depository institutions, also has a unique role in the platform, so the Governing Organization will form an advisory group to represent the interests of the Federal Reserve.

Unlike the ACH network, where financial institutions bear the financial risk of transactions they originate, a financial institution's role as depository and distributor of Fed notes does not inherently impose increased financial risk on participating depository institutions. Consequently, there is a lesser need for governance and advisory bodies to mitigate financial risk.

G.2.4, Proportionate Influence

The Solution’s governance approach should enable specific stakeholders or stakeholder groups to proportionately influence outcomes.

The Governing Organization has responsibility to ensure that representation within governance and advisory groups is both proportional and diverse. For example, large merchants (e.g., Walmart, Costco, Target, etc.) may be the receipt of a large number of payments; therefore, the
Governing Organization may form an advisory group to represent the proportional interest of any large stakeholder group. Additional advisory groups may be formed proportional to use or size of specific stakeholder groups.

**G.2.5, Conflicts of Interest**

The Solution’s governance approach should address and manage actual, perceived, or potential conflicts of interest.

The Governing Organization must manage actual, perceived, or potential conflicts of interest to protect the integrity of all Parties involved in governance arrangements and the overall integrity of the payment solution. The Governing Organization will establish processes and methods to identify, disclose, and manage actual, perceived, or potential conflicts of interest. One mechanism to avoid conflicts of interest is to disqualify members of the Board, executive team or staff members from participation in official matters. Another mechanism is to waive the conflict because participation of the members involved is more important to the process than resolving the conflict. All potential, perceived and actual conflicts of interest identified by any party will be discussed, documented, and appropriately disclosed to protect integrity of decision-making and governance arrangements.
**GLOSSARY OF TERMS**

The definitions for terms contained herein are defined in the context of this Solution Proposal. To be certain of the author’s intent, the definitions for terms herein are intended by the authors to augment the Glossary of Terms published by the Faster Payments Task Force.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Domain</td>
<td>The Internet domain under the control of the Federal Reserve where Federal Reserve notes are published, where participants may enroll to obtain a payment address in the Global Directory Service, and the location of the ledger of the end users holding Federal Reserve notes.</td>
</tr>
<tr>
<td>Central Bank</td>
<td>See “Issuer.”</td>
</tr>
<tr>
<td>Chain</td>
<td>A collection of payment addresses arranged together in a hierarchy where the root of the hierarchy provides a single, distinct name for all members of the hierarchy.</td>
</tr>
<tr>
<td>Closed-loop Currency</td>
<td>A national currency that is issued by a business in standard denominations that has various types of limits including expiration dates, amounts that can be held by individuals, whether or not it is transferable to other payment addresses, and payment addresses where it can be redeemed in exchange for goods and services.</td>
</tr>
<tr>
<td>Closed-loop Network</td>
<td>A group or collection of primary payment addresses that have all opted into, and agree to be governed by, a membership agreement that details the terms and conditions of membership and acceptance of the issuers’ brand cash.</td>
</tr>
<tr>
<td>Communication Channel</td>
<td>A medium and its associated methods of communicating with an end user.</td>
</tr>
<tr>
<td>Contextual Data</td>
<td>The information associated with the context of, related to, or surrounding a specific transfer.</td>
</tr>
<tr>
<td>Developer</td>
<td>A depository institution, regulated non-bank provider, third-party service provider or integrator that develops value-added features.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>An identification string that defines administrative autonomy, authority and control and is registered under the rules and procedures of the Domain Name System (DNS).</td>
</tr>
<tr>
<td>Domain Name Alias</td>
<td>The mapping of one domain name or part thereof (i.e., subdomain) to another.</td>
</tr>
<tr>
<td>Feature Certification</td>
<td>The process of testing and verifying value-added features before the feature is made available to end users.</td>
</tr>
<tr>
<td>Global Directory Service</td>
<td>A repository of searchable names and URL addresses that map to people and things.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Governing Organization</td>
<td>The executive officers, board of directors and board of advisors responsible for governing the Faster Payments Network.</td>
</tr>
<tr>
<td>Integrator</td>
<td>Depository institutions, regulated non-bank providers, and third-party service providers that develop value-added features.</td>
</tr>
<tr>
<td>Issuer</td>
<td>A central bank that provides financial and banking services for its country's government and commercial banking system, as well as implementing the government's monetary policy and issuing currency.</td>
</tr>
<tr>
<td>Holder</td>
<td>The end user enrolled in the FPN whose payment address is stored in the holder field on a Fed note.</td>
</tr>
<tr>
<td>OAuth2</td>
<td>An open standard for authorization design to work with HTTP providing a mechanism for authentication without sharing of credentials.</td>
</tr>
<tr>
<td>Open-loop Currency</td>
<td>A national currency issued by a central bank.</td>
</tr>
<tr>
<td>Payment</td>
<td>See “Transfer.”</td>
</tr>
<tr>
<td>Payment Address</td>
<td>A unique end-point (i.e., URL or URI) in the Global Directory Service controlled by one or more individuals or entities and accessed with credentials for authentication.</td>
</tr>
<tr>
<td>Payment Address Alias</td>
<td>Receipt of a pending transfer to a Payee through a communication channel (e.g., email, SMS/text, Social Media Post)</td>
</tr>
<tr>
<td>Payment Code</td>
<td>A random sequence of characters generated by the FPN that pre-authorize a transfer to a Payee.</td>
</tr>
<tr>
<td>Invitation</td>
<td>A message send by the FPN to a transfer recipient that does not have a payment address in the Global Directory Service.</td>
</tr>
<tr>
<td>Payment Order</td>
<td>The signed instructions from the Payer, submitted by the Payer or an individual authorized to act on Payer’s behalf, to the FPN for the execution of a transfer.</td>
</tr>
<tr>
<td>Possession Attribute</td>
<td>A databased record that contains the payment address of the holder of a Fed note.</td>
</tr>
<tr>
<td>Real-time</td>
<td>The combined speed of the computers and network over which the transfer request is processed and confirmation of completion provided to the Payer.</td>
</tr>
<tr>
<td>Standard Currencies</td>
<td>The officially recognized currencies found on the ISO 4217 currency code list.</td>
</tr>
<tr>
<td>Payment System</td>
<td>The Faster Payments Network presented in this solution proposal.</td>
</tr>
<tr>
<td>Person</td>
<td>Any individual.</td>
</tr>
<tr>
<td><strong>Stakeholder</strong></td>
<td>Any entity participating in the payment system including end users, Payers, Payees, providers, third-party providers, integrators, developers and central banks.</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>See “Payment System.”</td>
</tr>
<tr>
<td><strong>Transaction</strong></td>
<td>See “Transfer.”</td>
</tr>
<tr>
<td><strong>Transfer</strong></td>
<td>The update or change of the possession attribute on one or more Fed notes from one payment address in the Global Directory Service to another payment address in the Global Directory Service.</td>
</tr>
<tr>
<td><strong>Vanity URL</strong></td>
<td>A customized URL that is short, easy to remember, easy to use, and easy to share.</td>
</tr>
<tr>
<td><strong>Wallet</strong></td>
<td>An application developed by a third party that is used to effect payments.</td>
</tr>
</tbody>
</table>
Response to Faster Payments Network Assessment

This document answers the questions asked by the QIAT in the preliminary assessment of the Faster Payments Network solution proposal and provides additional details as requested by the QIAT. The information in this document supplements the solution proposal and is divided into five categories: implementation, scale, risk management, user experience, and governance. The table in the appendix at the end of this document provides cross-references of the QIAT’s questions with the section where the answer is provided in this document.

Implementation

This section includes information about participation requirements for providers, dependence on a mandate by the Fed, partnerships that could aid in the adoption of the FPN, feedback from users of the current open-source implementation, cross-border interoperability, and contextual data message formats.

Participation Requirements for Providers

Providers that choose to participate in the FPN do so under an agreement that outlines their participation requirements for distribution, deposits, information systems, and regulatory and legal requirements.

- **Distribution Requirements.** Consistent with the current responsibilities of depository institutions, depository institutions will have the responsibility to order, distribute and hold Fed notes on the FPN. Depository institutions should hold a sufficient supply of Fed notes to meet the demand for Fed notes on the FPN. To ensure an adequate supply, providers will order Fed notes on the FPN as needed; those orders will be fulfilled by authorized Fed personnel who have the responsibility to fill orders for Fed notes. An order for Fed notes will likely be filled from the existing supply of Fed notes but may trigger the creation of new Fed notes. The responsibility for distribution could be expanded under new rules to include non-bank account providers.

- **Deposit Requirements.** Providers must accept and honor Fed notes at face value, less any applicable deposit fee for deposit into an account with the provider. When a provider accepts Fed notes for deposit, the provider takes possession of the Fed notes and holds them until they are either returned to the Fed or requested by the provider’s customers.

- **Information System Requirements.** Providers directly connected to the FPN will be required to maintain their information systems up-to-date and consistent with published guidelines.

---

1 The “Participation Requirements for Providers” section provides further details as requested in S.11.
**Regulatory & Legal Requirements.** Providers will not inherit new regulatory requirements because of their role in the FPN. For example, providers will only have KYC and AML responsibilities for financial accounts held by their own customers. The provider will not have KYC requirements for individual payment addresses or transfers on the FPN between payment addresses unless the provider is either the Payer or Payee in the transfer.

Dependence on Mandate from the Federal Reserve

Implementation of the FPN is not dependent on a mandate from the Fed. Instead, the FPN would be operated by the Fed for the benefit of all consumers, businesses (including government organizations) and financial institutions. The Fed's operation of the FPN will provide credibility and trust in the FPN that only the Fed can provide. Financial institutions will be motivated to participate because financial institutions of all sizes will have a chance to compete against one another for distribution and deposits of Fed notes. Businesses are motivated to participate and receive all the benefits of payment in Fed notes. Businesses will use Brand cash to provide the motivation for consumers to participate in the FPN and pay with Fed notes.

Partnerships

The WingCash platform is succeeding in the market. It is being used by several parties on various initiatives, including one to lower the cost of cross-border remittances by 3-4 percentage points and another to provide new capabilities for promotion and branding utilizing brand cash; however, the relationships with these organizations would not be considered partnerships, nor would they be necessary if the FPN is adopted by the Faster Payments Task Force or Federal Reserve as the primary initiative for U.S. payment system improvement. There will be areas in the FPN where the Fed can provide functionality most efficiently by contracting with vendors, but those relationships would likely not be defined as partnerships.

The proposer believes that the Fed is able to provide sufficient, non-compulsory motivation to industry participants to adopt the FPN with or without partnerships from WingCash. For example, the Fed has demonstrated the ability to mobilize the industry with the establishment of the Faster Payments Task Force and Secure Payments Task Force. The membership of both task forces participate on a voluntary basis and not because of a mandate by the Fed.

Feedback from Current Users

WingCash has received positive feedback from business of all sizes, including large Fortune 100 companies, regarding their willingness to adopt the platform. We have also had discussions with members of management teams from large retailers that also participate on the Faster Payments Task Force. Our experience is that businesses respond quickly and affirmatively because, compared with payment card acceptance, the FPN offers significant benefits that large companies desire: transfers without fees, no requirement for specialized terminal equipment at the point-of-sale, no need to protect consumers’ personal information including payment card data, immediacy of payment including settlement, and the ability to deposit to existing accounts.

---

2 The “Dependence on Mandate from the Federal Reserve,” “Partnerships,” and “Feedback from Current Users” sections answer the questions asked in E.3.1.
with financial institutions. These features provide the benefits that large businesses want to see in a modernized, faster payments network.

In contrast to response from businesses, providers or depository institutions have been less accepting of the platform. Depository institutions, necessarily under regulatory scrutiny, are less willing to work with new payment platforms, particularly if the new platform could reduce the revenue associated with a financial institution’s fee income from ACH and, more significantly, payment cards.

The solution proposal’s approach is to have the FPN operated equitably by the Fed and GO for all Federal Reserve members and the public.

Cross-Border Interoperability

The Federal Reserve is the entity authorized to place United States Dollars into circulation. Adoption of the FPN by the Faster Payments Task Force and the Federal Reserve means that the Federal Reserve becomes a joint operator with the GO of an Internet-based system that allows, depending on the rules, individuals and entities (i.e., financial institutions, businesses and governments) around the world to hold and transfer United States Dollars on the FPN.

The proposer believes that the “heavy lifting” of the go-to-market plan for cross-border payments is established with the current confidence and trust placed in the US Dollar by other governments and institutions as a reserve currency. If the FPN is adopted by the Faster Payments Task Force and the Federal Reserve as the primary initiative for payment system improvement, then the primary responsibility of the organizations (i.e., the Fed, GO, implementation team, vendors) with roles and responsibilities for implementation of the FPN will be implementation with the highest levels of professionalism, care, oversight and responsibility so that the confidence and trust of the US dollar is maintained or even improved.

If the FPN provides the highest level of service for top U.S. retailers, that will be a huge step forward for cross-border implementation as well. For example, a successful deployment of the service by Walmart in United States may influence adoption by other countries where Walmart has operations.

Integration with Existing Payment Systems

While it is technically possible to have a separate instance of the FPN in every country, the Fed will likely control, jointly operate, and issue USD into only a single instance. Central banks or financial institutions in other countries may choose to operate an instance of the FPN in their country or to participate directly in the FPN operated by the Fed and the GO.

- Operating separate instances of the FPN in different countries. The FPN could be implemented directly into another payment network (e.g., Vocalink, FAST, SPEI, NPP)

---

3 The “Cross-Border Interoperability” section answers the questions asked in U.5.2, U.5.5, and E.4.2.
using its API, standard message formats and by implementing the necessary code changes in the FPN to support another payment network’s rules and regulations.

The technical design of the FPN supports workflows and multiple message formats. These features allow the FPN, as permitted by the rules, to interoperate with similar payment systems in other countries by implementing their standards for message formats, languages, regulations and settlement. For example, the current open source implementation inter-operates with both the ACH network and payment card networks in the United States.

It may be too cumbersome for the Fed to operate multiple instances of the FPN, as it would require significant effort to develop and maintain direct interoperability with systems throughout the world. However, for countries choosing to operate their own instance, interoperability is achievable by having at least one financial institution act as a gateway and/or exchange from one currency (USD) to another.

Instances of the FPN in other countries will support multiple languages, a selection of message formats and standards, and localized rules and regulation. The technical advantages of the FPN for settlement speed and efficiency are not eroded because an exchange or gateway processes through a financial institution.

- **Implementing a single instance of the FPN and allowing direct participation by other countries.** Compared with operating multiple instances of the FPN, it is relatively simple to allow the operators of payment networks in other countries to interoperate using the FPN’s API and standard message formats according to the rules and regulations of the FPN.

Support for cross-border transfers are being added to the current open-source implementation using International ACH (IAT) transfers, making it possible to transfer funds to accounts in other countries.

The proposer believes that other countries will choose, as FPN rules permit, to integrate with the FPN using the FPN’s API and published standards. The FPN can support either of the flows above because of its flexible workflow engine and technical design.

**Contextual Data Message Formats**

The JSON format is one example of a structured format (see RFC 7159). If it is determined that it is to be one of the supported message formats at implementation, then a schema definition with a revision number should be included to provide information about the structure (e.g., field names, types and attributes) of the messages being served. The technical design makes it possible to serve contextual data in JSON, XML, or another format that the implementation team determines should be supported. The FPN is capable of serving any standard format, such as XML.

---

4 The “Contextual Data Message Formats” section answers the question asked in E.4.1.
ISO 20022 is an XML-based message format; consequently, there is no performance risk in relying on data transformations to ISO 20022 and no need to plan for mitigating factors.

Scale\(^5\)

The Strategies for Improving the US Payment System paper published by the Federal Reserve System indicates that the “faster payments analysis demonstrated that increased payment speed would initially benefit at least 29 billion transactions per year, which is 12 percent of the total for the country.”\(^6\) However, the footnote on page 10 of the paper indicates that 29 billion does not include “latent demand that might materialize” or “point-of-sale transactions,” which the proposers intend should be served at launch.\(^7\)

The Proposers have tested the transaction throughput of the current open source version without much code optimization using Amazon EC2 Type C3 instances with 32 cores and 60 GiB of memory. The current open source version was able to achieve projected annual transaction throughput rate in excess of 23 billion transfers per year (750 transactions per second, 64.8 million transactions per day). To put this in perspective, VocalLink, the operator of the UK’s Faster Payments system, indicates on their website that their data centers process just over 6 billion BACS transactions annually (16.44 million per day), with a peak reaching 100 million transactions per day (36.5 billion transactions annually). The proposers believe that, with both hardware and software optimizations, the transaction throughput of the FPN at implementation can be improved to reach or exceed 220+ billion transfers per year, or 602.7 million transfers per day. The FPN’s architecture is designed to accommodate growth with additional code optimization and through horizontal scale.

The FPN will create and store data for each Fed note on the FPN. While this may seem like a lot of data, even with billions of Fed notes, it is rather small by comparison. YouTube reports that “every day people watch hundreds of millions of hours on YouTube and generate billions of views.”\(^8\) The processing demand to serve hundreds of millions of hours of YouTube video is an activity that has a high demand on computing resources (i.e., computer processing power, network bandwidth, and storage), whereas the FPN’s serving static/dynamic web pages demands much less computing resources.

The FPN can scale quickly while maintaining service level agreements and providing the baseline core features because of an original design architecture that supports high scalability.

When we conceived of the solution in 2009, we recognized the need for high scalability. We knew from experience that the eventual bottleneck in most Internet-scale projects is the large central database at their core. Although modern databases are remarkably fast, at some point

---

\(^5\) The “Scale” section contains responses to the questions asked in E.6.2.  
\(^6\) The Federal System, Strategies for Improving the US Payment System, 26 January 2015. P. 10  
\(^7\) See Faster Payments Network Solution Proposal, Section C, Efficiency, E.3.1, Credible Plan to Achieve Implementation by 2018 and Ubiquity by 2020.  
the demand for more storage and faster queries exceeds the capacity of current hardware. We also knew we should build on well-tested database technology supported by many companies.

We designed and built for high scalability by basing the FPN’s architecture on application-level sharding, which means we store the data in distributed databases rather than a single central database. To support movement of data between databases, the solution uses persistent message queuing (with many independent queue servers), auditable logs of all note movement, and carefully chosen locking mechanisms. By spreading the data among many databases, the FPN can scale by adding commodity hardware instead of more expensive high end servers.

An interesting example of the use of application-level sharding is the way the FPN transfers possession of Fed notes from one user to another, even when the user records are stored in different databases. Let's say there are 4 databases:

- D1 stores the permanent record of a Fed note.
- D2 stores the list of Fed notes held by user U
- D3 stores the list of Fed notes held by business B
- D4 stores a list of transfers between users.

When user U wants to send a $1 Fed note she holds to business B, the FPN follows these steps:

- A front-end server sends a message to any available transfer server, passing the attributes of a new transfer to execute.
- The next available transfer server creates a transfer in database D4. The new transfer has a sender ID, recipient ID, start time, an amount, a currency code, and a transfer ID.
- The transfer worker asks database D2 for a Fed note from user U.
- Assuming a Fed note is available, that Fed note is marked as unavailable in database D2 and the Fed note is added to the transfer. The transfer is now the temporary holder of the Fed note; no other transfer can take possession of the Fed note. User U no longer has control of the Fed note.
- The transfer server tells database D3 to assign business B as the holder of the Fed note.
- The transfer server tells database D2 to remove the Fed note from U and tells database D3 to release the Fed note to business B. At this point, business B is in possession of the Fed note and may send it to someone else.
- Each of the above steps is recorded in D4 as they happen. All involved stakeholders may be permitted to see all or portions of the transfer log.
These steps become more complex when the transfer become more complex; however, the basic architecture has remained intact throughout the years of product development and demonstrates that the FPN is highly scalable because of the use of application-level sharding in the technical design from inception.

Ensuring Resiliency at Scale

Resiliency is achieved at scale by ongoing efforts to mitigate common threats to ensure high availability and security against cyber-attacks. The following are examples of common threats and how the FPN prevents and responds to these attacks to achieve resiliency:

- **Hardware theft.** To prevent hardware theft and the theft of stored data, the following measures mitigate the impact of hardware theft attack:
  - All FPN applications and servers are operated in a secure facility with limited, controlled access.
  - The FPN encrypts all data at rest using strong encryption so if hardware is stolen, stored data is not recoverable.
  - The FPN maintains automatic, offsite backups of all data so that data is preserved even if hardware is stolen or destroyed.

- **Operating system vulnerabilities.** Security issues are regularly discovered in all operating systems and to mitigate the impact of operating system vulnerability the following measures are taken:
  - Patches are tested and applied promptly with minimal human intervention.
  - To ensure patches do not break the software, all servers are built using an automated system configuration system that keeps per-server settings correct.
  - The FPN will apply per-process restrictions using a system called AppArmor, limiting the possible damage from any unknown vulnerabilities.

- **External network attacks.** To mitigate the impact of external network attacks the following measures are taken:
  - Because attackers often try to connect to database servers directly through network ports, the FPN employs external firewalls that reject all attempts to connect to non-public ports.
  - The FPN mitigates denial of service (DoS) attacks by providing flexible server capacity and by adjusting firewall rules in real-time to temporarily block specific abusive IP addresses.
  - The FPN serves static copies of web pages in the event of an extreme DoS attack. Because copies of static web pages require few server resources, it is more difficult for attackers to overwhelm servers that serve static copies of web pages.
  - The proposers recommend the creation of a site reliability engineering (SRE) team to monitor the network and build automated detection and response systems.

---

9 The “Ensuring Resiliency at Scale” section contains responses to the questions asked in S.8.1.
• **Internal network attacks.** Sometimes attackers access internal physical networks, such as by compromising an Ethernet switch or adding an extra device to the network to connect directly to database servers. The following measures can mitigate the impact of internal network attacks:
  o The FPN employs internal firewalls that reject and report all attempts to connect between servers in unexpected ways.
  o The FPN authenticates and encrypts internal connections between servers, preventing unauthorized access even by people who can plug a device directly into the internal physical network.
  o The FPN will maintain centralized logs of all server activity. The logs will be audited for suspicious behavior.

• **Administrative attacks.** Sometimes attackers try to impersonate someone with administrative or software development access. The following measures can mitigate the impact of administrative attacks:
  o The FPN employs a VPN; VPN access is required for all administrative and software development access.
  o All administrators and developers must use personal credentials over TLS or SSH connections (layered over the VPN connection).
  o The FPN holds a small database of all currently authorized administrators and software developers. When someone no longer needs access, they are promptly removed from the access control list.
  o Administrators have only the privileges they need to do their jobs.

• **Attacks by software developers.** Sometimes software developers add security vulnerabilities, either unintentionally or intentionally. The following measures can mitigate the threat of attack by software developers:
  o The FPN requires regular, independent code reviews. Code reviewers look for any kind of security vulnerability.
  o All software and configuration is kept in a version control system that maintains a complete history of all changes. Software developers do not have the ability to manipulate version control system and history and all deployed software passes through the version control system. Consequently, evidence of vulnerabilities added by software developers is permanent.

• **Advanced persistent threats.** Large companies have recently become aware of people gaining unauthorized, undetected access to their systems through undiscovered vulnerabilities in software and hardware. To detect manipulation by someone who defeats all other defenses, the FPN will employ an auditing system. The auditing system will regularly receive encrypted copies of all data stored by the FPN. The auditing system will be disconnected from the Internet and will ensure the FPN always follows certain rules, such as:
  o Many attributes of notes must never change, such as the value, currency, note ID, and issuer ID.
  o Existing transfer steps must never be removed or changed.
○ Each Fed note has a holder ID, and each holder has a list of Fed notes he or she holds; those two pieces of information must always agree.
○ Transfers that have been completed must never continue to hold Fed notes.
○ Transfers must be completed within a reasonable amount of time (depending on the transfer type).

While this list is not comprehensive, the FPN will need to employ measures like those listed above to achieve resiliency and to mitigate the threat of cyber-attacks. Measures like these are taken by organizations like Amazon, Google, Facebook, and Apple, which operate services that require resiliency and high availability.

Risk Management\(^{10}\)

The rules, policies and procedures addressing operational and information security risk for the FPN will need to be broad-based and comprehensive. The FPN is primarily an information system, so operational risk related to information security will be vitally important at implementation and on an ongoing basis as payments are switched from other payment networks to the FPN. The FPN will be a system of both high interest and high impact nationally and perhaps even globally. Consequently, the Risk Management Framework (RMF) will be fully developed by the GO, the implementation team, and the Secure Payments Task Force, with input and approval by the Fed. The National Institute of Standard and Technology develops and publishes guidance and courses for organizations to develop broad-based, comprehensive, organization-wide RMF.\(^{11}\) The comprehensive RMF needed for the FPN will include risk operational and information security policies for the GO (its board, executives, managers, staff and membership), the FPN and related information systems (e.g., those provided by vendors).

Fraud Prevention and Remediation\(^{12}\)

The FPN’s focus on fraud prevention instead of remediation will not require businesses and governments to adopt special protective measures to guard against fraud. The FPN establishes equality and balance among stakeholders and addresses important concerns for Payers and Payees. For outbound payments, businesses and governments will be concerned that payments are authorized by the appropriate people within the organization before the payment is processed. To address this important concern, the FPN can require that a payment is signed by two authorized individuals (e.g., CFO, treasurer) before the payment is processed. In this way, the FPN can be used by businesses and governments to replace slower, less efficient forms of payment, such as checks. Other important concerns for businesses and governments addressed by the FPN’s technical design include the ability of the FPN to a) identify each payment uniquely, b) identify and record the individuals within the organization who authorized each payment, c) track source and destination of all payments, d) send notifications of payments to all individuals who authorized the payment, e) allow authorized individuals to audit

\(^{10}\) The “Risk Management” section answers the question asked in S.1.3.

\(^{11}\) National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center.

\(^{12}\) The “Fraud Prevention and Remediation” section answers the question asked in S.5.4.
all payments and the payments details, and e) allow for either manual or automated reconciliation of all payments through existing accounting systems.

Because the FPN focuses on fraud prevention by making the Payer accountable for transfers, businesses and governments should also feel confident that they will not receive fraudulent payments from customers, as Payers will likely not send money unless the business or government entity is expecting payment.

Handling Exceptions

The FPN will use a combination of tools to identify and repair exceptions in a reasonable time frame. For example, the Simple Network Management Protocol (SNMP) is an application layer protocol that allows the changes status of all network applications (e.g., front-ends, message queues, transfer servers, etc.) to be monitored in real time. While SNMP support will be built into each of the network servers, the actual software application that receives the traps and shows the network map and status of all the servers will be developed by and licensed from a software vendor (e.g., Ipswitch, Nagios, etc.).

The FPN also includes a back-end administrative tool that has already been developed. The Fed and the GO will be able to use the administrative tool to identify and resolve transfer errors, failed signup attempts, canceled payment addresses and more. It can also be used to audit note holders and transfers and to check transfers that are set to execute at a certain time.

The FPN captures exceptions data and transfer errors in a centralized logging repository. The centralized log can be analyzed using data analysis tools and/or programing languages, such as Python, to spot exception patterns.

When an exception pattern has been identified, the GO and those responsible for managing the FPN’s operations will need to analyze the exceptions data, then determine, develop and implement the correct response for handling the exceptions.

For example, the fraud detection group may discover a common pattern of individuals transferring small amounts among many payment addresses to hide the possession history, then aggregating the value into a single payment address to be spent or deposited into an account at a depository institution. In response to detecting this sort of pattern, the fraud detection group could write and implement processes and procedures to suspend payment addresses that are participating in the detected pattern. Suspended payment addresses could then be evaluated and investigated.

User Experience

User experience refers to the experience of persons and entities who are using the FPN. This section provides information about authorizing multiple users to make payments, resolving disputed payments, message formats, contextual data, and payment codes.

---

13 The “Handling Exceptions” section answers the questions asked in E.7.1 and E.7.3.
Authorizing Multiple Users to Make Payments\textsuperscript{14}

A Payer is a person who is authorized, using his/her own credential, to initiate a payment from a payment address.

A payment address must have at least one and may have more than one credential (i.e., authorized Payers) associated with it. For example, the payment address for a business (e.g., Zions Cafe) does not have its own credential on the FPN. Rather, a person, in this case Sam the owner, enrolls the business using his personal credentials. Because Sam created the business, his credential is associated with the Zions Cafe payment address as the manager. As the manager, he can assign permissions to other persons to act on behalf of the business using their own credentials. Individuals must use valid credentials to enroll, manage, or authorize payment orders for a business payment address and to delegate authority to other users. The FPN has a role-based permission system that grants differentiated access to information, and it allows more than a single individual to be assigned to a given role.

The FPN’s technical design also permits personal payment addresses to have multiple credentials associated with a single payment address. For example, a father can establish a payment address for his daughter. Although the daughter accesses the payment address with her own credential, the father is also able to switch to or proxy the daughter's payment address using his own credential. The process of proxying a payment address is similar to changing from a personal to a business page on Facebook.

The FPN records, logs, and tracks all activity for a business payment address by user. In addition, the FPN has access control for activity feeds that is restricted by a secret key embedded in the subscription URL and IP address. Only appropriate users can view and change the secret keys used to access activity feeds.

The FPN enables persons with management credentials to require second-factor authentication (such as biometric or hardware token authentication) for some use cases. It can also require end user re-authentication at various points in a payment cycle, such as when a user proxies from a personal to a business payment address or submits a payment.

Disputed Payments\textsuperscript{15}

The purpose of the FPN is to provide Payers and Payees with a reliable method for electronic receipt of a final payment. In so doing, the FPN’s technical design adheres to, and functionally preserves, principles of payment found in the use of physical banknotes and coins, including where there is not an intermediary appointed (i.e., depository institution) to act on behalf of either the Payer or Payee in resolving a dispute. Consumers and businesses are aware of their recourse rights under ACH and payment card rules and the law. The FPN’s technical design has been carefully architected using specific design principles to address reasons for dispute through an appointed intermediary (e.g., depository institution, GO, Fed) as exists today with the

\textsuperscript{14} The “Authorizing Multiple Users to Make Payments” section answers the question asked in L.2.4.
\textsuperscript{15} The “Disputed Payments” section answers the questions asked in S.3.3 and S.5.1.
ACH and payment card networks. The design principles of the FPN that mitigate the need for an intermediary to resolve disputed payments include: a) all transfers are push-only payments with authorization by the Payer using a verified identity and valid credential for each transfer; b) transfers do not include the Payer’s identity or account information, which limits the opportunity for abuse by the Payee; c) the Payer has a choice of payment methods and can choose not to use the FPN for certain payments or with certain Payees; d) the transfer provides the Payer and Payee with visibility and transparency of the payment; and e) the transfer provides privacy for both the Payer and Payee.

If a Payer has a payment dispute, he or she will have recourse available under the FPN’s rules, applicable regulation, and the law for disputing payments. The FPN will have rules and regulations as established and approved by the members of the GO to protect Payers. The FPN’s architecture does not limit legal rights of Payers to dispute payments through applicable channels.

- A Payer has the option to first work with the Payee to resolve the dispute.
- In the event of failure to resolve the dispute directly with the Payee, the Payer has options for dispute resolution provided as part of the FPN’s rules and/or regulations.
- In the case where the FPN’s rules do not satisfy the Payer, the Payer may have rights to dispute the under the law.

Message Formats

The FPN’s technical design allows for transfer and contextual data to be served in more than a single message format but conforms to standard message formats. As demonstrated with the current open-source implementation, a transfer with its associated contextual data is served as a webpage using a combination format of HTML5, Cascading Style Sheets and JavaScript. An authenticated end user or stakeholder can display the message using any web browser to access the transfer URL (e.g., https://fednotes.net/transfer/12274-74710340). The end user or a computer program can access the same transfer and contextual data on computer-friendly JSON or XML formats by visiting different end-points (e.g., https://fednotes.net/transfer/12274-74710340/json or http://fednotes.net/transfer/12274-74710340/xml).

Enabling Updates to Standard Message Formats

The FPN provides two mechanisms for updates to standard message formats (e.g., JSON, XML):

- **Versioning.** Versioning of standard message formats is achieved by updating message format documentation and referencing the version within a response. An example of versioning is found in the API documentation for the open source implementation (see wingcash.com/api). The documentation for the API refers to the response message and describes the fields and attributes included in the response. To maintain stability, we

---

16 The “Message Formats” section answers the question asked in E.4.3.
17 The “Enabling Updates to Standard Message Formats” section answers the questions asked in U.4.3 and E.4.4.
prefer to add new fields and attributes before changing or removing existing fields and attributes. We do expect that over time functions, fields, and attributes will change and some will even be deprecated or removed.

- **Schemas.** Another proven mechanism to enable updates to a standard message format is to define and include a formal schema definition. The FPN can serve data in JSON format, XML format or potentially another supported format. When the data is served, it can include a reference at the top of a message to the schema and its revision number (e.g., https://api.fednotes.net/schema/json/ver1221 or https://api.fednotes.net/schema/xml/ver2341). In this way, the consumer of the message will receive not only the data but also a link to access the schema which can be used to validate the data. The example below shows how a schema reference is included in the response of a JSON message.

```json
{
  "$schema": "https://fednotes.net/schema/json/ver1221",
  "activity_count": 14,
  "amount": "29.05",
  "canceled": false,
  "completed": true,
  "currency": "USD",
  "end": "2016-08-15T21:34:19.184522+00:00",
  "id": "17044616460",
  "loyalty": [],
  "next_activity": "completed",
  "payment_details": [],
  "posts": [
    {
      "action": "split",
      "id": "13751196435",
      "private": true,
      "timestamp": "2016-08-15T21:34:18.651341+00:00",
      "transfer_id": "17044616460",
      "transfer_url": "https://www1255594483.wingoash.org/t/17044616460",
      "url": "https://www1255594483.wingoash.org/2m69Xx/"
    },
    {
      "action": "send",
      "id": "15991958232",
      "private": true,
      "timestamp": "2016-08-15T21:34:19.006007+00:00",
      "transfer_id": "17044616460",
      "transfer_url": "https://www1255594483.wingoash.org/t/17044616460",
      "url": "https://www1255594483.wingoash.org/2119hrs/"
    }
  ],
}
```

The use of multiple end-points for serving transfer and contextual data information makes the FPN flexible and adaptable to the future and changes in technology. The GO, working with its members, will determine what message formats will be implemented and the process, procedure and timing of migration to updated and or new message formats.
Contextual Data

The FPN enables flexibility in contextual data as follows:

- Allowing end users to add contextual data in both unstructured (e.g., text) and structured formats (e.g., JSON, XML, XSN.1).
- Allowing end users to define the structure (i.e., schema, data dictionary) for certain fields and add contextual data for all supported use cases, including business payments.
- Allowing end users multiple methods of consuming contextual data, including data feeds, web pages, and an API.

The FPN has defined certain fields for use in its data dictionary; however, the FPN’s technical design does not limit end users to the use of this specific data dictionary with business payments; instead the FPN’s technical design supports data fields across the spectrum, from a custom-defined data dictionary defined by a specific end user to the data fields included in an open standard like ISO 20022. The Fed, the GO, and its members should determine the actual message formats and associated data dictionaries to be supported at implementation. End users will then determine how they want to use the data dictionary and structured format in certain data fields in the FPN.

Flexibility Through Workflows

The FPN also achieves flexibility in contextual data by being built on the concept of workflows. At a high level, a workflow is a series of actions conducted by computers and/or humans, where each action is recorded permanently. Actions can include updating database tables, storing contextual data in the workflow, notifying people by email or SMS, waiting for human interaction, waiting for an external computer system, or starting a new workflow.

The FPN treats every monetary transfer as a workflow. Each transfer follows a predefined series of actions based on the transfer type. The first action of the transfer workflow records the initiating user's intent. For simple "send" transfers, the first action records the sender ID, recipient ID, amount, and currency. For more complex transfers, the first step records more information. For example, when a user sends money to a bank account, the first action is to record any deposit fees.

The transfer maintains a simple key/value mapping of contextual transfer data. Each action in the transfer updates values appropriate for that action. The keys are field names as specified in the design, and the values are strings of any reasonable size. Values may contain any kind of data, such as numbers, JSON, XML, or binary content. The transfer also maintains an immutable history of changes to the transfer data.

Monetary transfers in the FPN tie together many pieces of information that are often disjointed in banking and accounting software. For example, if a transfer communicates with an external system...

---

18 The “Contextual Data” section answers the questions in U.4.1.
19 The “Flexibility Through Workflows” section answers the question asked in U.4.3.
system such as a foreign bank, a transfer action records that interaction in the transfer data, and the FPN can make that interaction visible in the history.

The workflow does not replace double-entry accounting tables; it enhances and simplifies them. One pattern the proposer has discovered is that when a transfer adds an entry to an accounting table, the accounting table should link back to the transfer. This way, the accounting table needs only one field for supporting information; the transfer can store any helpful information and justification without complicating other tables.

The FPN supports aggregate queries of transfers so that software can analyze them in batches. The FPN will also support downloading transfer information in formats supported by common accounting software (e.g., CSV, TXT delimited, QIF, QFX, QBO, and OFX).

The following examples illustrate the steps in the workflow. (See “Show Steps” section in each example.)

---

**Transfer Details**

<table>
<thead>
<tr>
<th>Transfer ID</th>
<th>1647-2824-214</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Send</td>
</tr>
<tr>
<td>Start</td>
<td>Monday, 15 August 2016 4:00:19 PM (less than a minute ago)</td>
</tr>
<tr>
<td>End</td>
<td>Monday, 15 August 2016 4:00:19 PM (less than a minute ago)</td>
</tr>
<tr>
<td>Status</td>
<td>Completed</td>
</tr>
<tr>
<td>Amount</td>
<td>USD $1.00</td>
</tr>
<tr>
<td>Participants</td>
<td>Bradley Wilkes (Sender)</td>
</tr>
<tr>
<td></td>
<td>Cody Wilson (Recipient)</td>
</tr>
<tr>
<td></td>
<td>Federal Reserve Bank of Chicago (Provider)</td>
</tr>
<tr>
<td>Visibility</td>
<td>Restricted</td>
</tr>
<tr>
<td>Sender IP</td>
<td>50.160.82.41</td>
</tr>
</tbody>
</table>

---

**Steps of the workflow shown from here down**

1. On Monday, 15 August 2016 (less than a minute ago), Bradley Wilkes initiated a transfer of USD $1.00 ($1.00 United States dollars) to Cody Wilson with the message: Demonstrating a simple workflow with a $1 transfer.
2. Bradley Wilkes offered the exact amount.
3. Cody Wilson received the cash.
4. WingCash notified Bradley Wilkes by email that the transfer has completed.
5. WingCash notified Cody Wilson by email that the transfer has completed.

---

*Workflow example transfer 1647-2824-214 of $1 to another person with a text message included for the Payee formatted for viewing with a web browser (simple workflow)*
Workflow example transfer 1363-7595-533 a $100 deposit to an account at a financial institution showing a surcharge deposit fee of $.25. (more complex workflow)

You can click the links below to see the same workflow example transfers shown above, except formatted in JSON to illustrate how the contextual data in the workflow is formatted for computers or applications to read:

- Transfer 1647-2824-214 of $1 to another person with a text message also shown formatted in JSON (simple workflow)
- Transfer 1363-7595-533 a $100 deposit to an account at a financial institution showing a surcharge deposit fee of $.25. (more complex workflow)
Integrating Contextual Data into External Systems

The FPN is an external system to a treasury workstation or consumer accounting software. The FPN supports integration with external systems by providing the following:

- Assigning of a globally unique identifier for each transfer that can be expanded into a valid hyperlink on the FPN for the delivery of both transfer and contextual data (e.g., https://fednotes.net/transfer/12274-74710340 or https://fednotes.net/transfer/12274-74710340/json).
- Making it possible for end users to apply tags, category names and/or group names to individual transfers.
- Making it possible for the end users to store associated contextual data in certain data fields in the end user’s choice of formats from simple text to more structured formats (e.g., JSON, XML) using the end user’s own defined data dictionary for use by an external system.

The foregoing features make it possible for external systems to integrate transfer and contextual data across the spectrum from manual recording by people to automated integration by computer systems and software.

Example of Integration with Consumer Accounting Software

The following is an example of manually integrating transfer and contextual data information from the FPN into an external account system (e.g., QuickBooks):

Sam is the owner of Zions Cafe, a single location cafe. Twice each week he receives a delivery of various restaurant supplies from Sysco. He pays for the supplies on delivery using the FPN. After making the payment, he tags the transfer with the names of the appropriate expense accounts so that he’s reminded which accounts he wants to use in QuickBooks when recording the expenses. When Sam records the expense in QuickBooks, he reduces a different current assets account called “Fed notes” and increases an expense account called “restaurant supplies.” Sam records the transfer ID, 1374-7471-340, and the vendor, “Sysco,” with this entry in QuickBooks. The integration for this specific transfer in QuickBooks is complete.

The same example described above can also be automated by Intuit, the developer of QuickBooks. In the automated example, Sam follows the same procedure for making the payment to Sysco at the time of delivery and tagging the appropriate expense category. At any time during the month, Sam can now open QuickBooks and, using the business profile address (e.g., fednotes.net/zionscafe), he can tell QuickBooks go get transfer details and automatically create the appropriate entries.

20 The “Integrating Contextual Data into External Systems” section provides the details requested for U.4.2.
The same features that make it possible for Intuit to integrate QuickBooks for Zions Cafe also make it possible for developers of treasury workstation to automate the integration of treasury workstation software and many other types of software with the FPN.

Payment Codes\(^{21}\)

Payment codes allow the Payer to pre-approve or pre-authorize a specific amount of money to be spent with a specific Payee (i.e., payment address or chain) within a specified period of time (e.g., 30 minutes, 1 hour, 1 day, 30 days). Although not available in the current open-source implementation, the pre-authorization features may be enhanced to allow the Payee to pre-authorize a payment for a future date.

The FPN's current technical design allows the Payee only a single validation of a randomly generated payment code. Thus, as currently designed, payment codes can be used for recurring payments; however, the Payer is required to authorize each successive payment by presenting a unique, unused payment code to the Payee.

Note: The FPN solution proposal includes a mistake in the link to the demonstration video. The link points to P2P Use Case - Remote Payments. The correct link is to Create, Modify, or Cancel Payment Codes.

Governance

This section outlines the composition of the governing organization (GO), the rule- and decision-making processes, and how the GO will handle conflicts of interest.

Composition of the Governing Organization\(^{22}\)

The proposer recommends that the membership of the GO be broadly composed to include representation from all FPN stakeholders individually and collectively. For example, because depository institutions distribute Fed notes, depository institutions should be members of the GO and have a vote in the rules. However, unlike the governance of the ACH network, where membership is primarily limited to depository institutions, the membership of the GO should be expanded to include members from other stakeholder groups, including members from government organizations and businesses with a variety of structures (e.g., C corp, S corp, partnership, cooperative, LLC, association) and of various sizes, and offering a variety of products and services. The membership may also allow individuals to join, participate in committees and have a vote on rules. Individuals representing organizations may also be grouped into market segments, following the pattern of the current Faster Payments and Secure Payments Task Forces.

\(^{21}\) The “Payment Codes” section answers the questions asked in S.2.2.  
\(^{22}\) The “Composition of the Governing Organization” section answers one of the questions asked in G.1.1.
Making Decisions and Rules

The proposer recommends applying the decision-making framework established, adopted and operated by Faster Payments Task Force (FPTF) to the process of rule-making for the GO. The decision-making framework can be appropriately modified and amended as necessary for the adoption of rules by the GO. The decision-making and rule-making frameworks will be part of the ongoing process to establish rules for the FPN. Because the members of the FPTF have worked through updates and changes to the decision-making framework, they are well prepared to work through the adoption of the rules for the FPN.

Stakeholders will have a proportional influence on outcomes by being able to cast a vote for or against both decisions and the motion to adopt or change rules. In the current proportional representation system of the decision-making framework of the FPTF, stakeholders cast both individual votes and market segment votes (e.g., large financial institutions, medium financial institutions, business end users). A decision or rules adoption or change must receive two-thirds or more of the GO voting membership and a majority in at least six of the eight market segments to achieve majority consent. The use of FPTF decision-making framework allows for diverse representation of the GO’s membership to influence the adoption of decisions and rules.

Managing Conflicts of Interest

The GO can expect “traditional” conflicts of interest to arise where a member of the board of directors or a member of the executive team who has the ability to influence or direct the fiscal resources of the GO has a say in the process. For example, a member of the executive team of the GO is also an owner in an organization that has a contract to provide independent audit services to the GO. The conflict should be disclosed to the GO, and, at a minimum, the executive with ownership in the independent audit services firm should recuse himself/herself from the process that involves selection of the organization to be awarded the audit contract.

The GO is a unique governance body with participation from member stakeholders representing both consumers and every industry segment. While NACHA is an approximation of this form of governance, it is different because only financial institutions have a vote in NACHA rules. The payment card networks are corporations, and rule-making is not performed by a vote of the membership.

---

23 The “Making Decisions and Rules” section answers one of the questions asked in G.1.1 and the question in G.2.4.


26 The “Managing Conflicts of Interest” section answers the questions asked in G.2.5.
# Appendix: Questions for Proposers

This section includes the questions and requests for details presented by the QIAT in their preliminary assessment after their review of the Faster Payments Network solution proposal, along with references to where each question is answered within this document.

<table>
<thead>
<tr>
<th>Section</th>
<th>Questions/Requests for Detail</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ubiquity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.4.1</td>
<td>What is the message format used for contextual data? What data fields are available for business payments?</td>
<td>Contextual Data</td>
</tr>
<tr>
<td>U.4.2</td>
<td>Please provide an example of how the Solution can integrate contextual data with a Treasury workstation or Consumer accounting software, etc.</td>
<td>Integrating Contextual Data into External Systems</td>
</tr>
<tr>
<td>U.4.3</td>
<td>How does the Solution provide flexibility in the contextual data? How are data fields changed?</td>
<td>Flexibility Through Workflows, Enabling Updates to Standard Message Formats</td>
</tr>
<tr>
<td>U.5.2</td>
<td>How does the Solution allow for interoperability with similar Payment Systems in other countries accounting for differences in messaging standards, languages, regulations, settlement)?</td>
<td>Cross-Border Interoperability</td>
</tr>
<tr>
<td>U.5.5</td>
<td>What is the plan for achieving cross-border payments to other countries (go-to-market plan for adoption from other countries or interoperability with their payment systems)?</td>
<td>Cross-Border Interoperability</td>
</tr>
<tr>
<td><strong>Efficiency</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.3.1</td>
<td>What feedback has WingCash received from Providers and businesses on adopting WingCash, whether in the U.S. or based on experience in other countries? What partnerships are in place for adoption of WingCash? How dependent is the implementation plan on a mandate from the Federal Reserve?</td>
<td>Feedback from Current Users, Partnerships, Dependence on Mandate from the Federal Reserve</td>
</tr>
<tr>
<td>E.4.1</td>
<td>How does the JSON message format support the contextual data requirements of business payments? What are the performance risks and mitigating factors to reliance on data transformations to ISO20022?</td>
<td>Contextual Data Message Formats</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>E.4.2</td>
<td>How does the FPN’s technical design enable cross-border interoperability?</td>
<td>Cross-Border Interoperability</td>
</tr>
<tr>
<td>E.4.3</td>
<td>How are standard messaging and communication protocols (U.3.3) achieved if integrators have their choice of message format?</td>
<td>Message Formats</td>
</tr>
<tr>
<td>E.4.4</td>
<td>How does the Solution enable a mechanism of updates to the JSON message format?</td>
<td>Enabling Updates to Standard Message Formats</td>
</tr>
<tr>
<td>E.6.2</td>
<td>What are the projected volume and values that the Solution will need to handle? How quickly and to what levels can the Solution scale while still maintaining its SLAs / baseline core features?</td>
<td>Scale</td>
</tr>
<tr>
<td>E.7.1</td>
<td>What tools are provided to support the ability to work together to repair or otherwise address exceptions in a reasonable time frame?</td>
<td>Handling Exceptions</td>
</tr>
<tr>
<td>E.7.3</td>
<td>What does the Solution plan to implement around aggregation of exceptions data to spot patterns? What will the Solution do in response to pattern detection?</td>
<td>Handling Exceptions</td>
</tr>
</tbody>
</table>

**Safety and Security**

<p>| S.1.3  | What is the risk management framework (rules, policies, and procedures)? In particular, what are the rules, policies and procedures addressing operational risk? | Risk Management |
| S.2.2  | How do payment codes function as pre-authorization? Can recurring payments be set up using the payment codes? | Payment Codes |
| S.3.3  | What options/recourse does a Payer have if there is a payment dispute? | Disputed Payments |
| S.5.1  | What options does a Payer have if there is a payment dispute (S.3)? | Disputed Payments |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Question</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.5.4</td>
<td>As the proposer’s approach to fraud is more focused on prevention than remediation, will businesses and governments require more protections to adopt the solution?</td>
<td>Fraud Prevention and Remediation</td>
</tr>
<tr>
<td>S.8.1</td>
<td>Are there past examples or models of resiliency at the scale required for WingCash to succeed that would provide confidence in the ability to ensure high availability and security against cyber-attacks?</td>
<td>Ensuring Resiliency at Scale</td>
</tr>
<tr>
<td>S.11</td>
<td>Please provide further details, if any, on the Participation Requirements.</td>
<td>Participation Requirements for Providers</td>
</tr>
</tbody>
</table>

**Speed (Fast)**

No questions

**Legal**

<table>
<thead>
<tr>
<th>Section</th>
<th>Question</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.2.4</td>
<td>The FPN rules permit only the Payer using valid credentials to act on its own behalf to send payments, but the technical design enables a person to safely authorize another person to send payments. How will the FPN be implemented on this issue?</td>
<td>Authorizing Multiple Users to Make Payments</td>
</tr>
</tbody>
</table>

**Governance**

<table>
<thead>
<tr>
<th>Section</th>
<th>Question</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1.1</td>
<td>What will be the composition of the Governing Organization?</td>
<td>Composition of the Governing Organization</td>
</tr>
<tr>
<td>G.1.1</td>
<td>Per the proposal, rule changes can be proposed by any individual member, business or corporate member, or affiliate member or partner. What would be the rule-making / decision-making process?</td>
<td>Making Decisions and Rules</td>
</tr>
<tr>
<td>G.2.4</td>
<td>What are the ways in which specific stakeholders would be able to proportionately influence outcomes?</td>
<td>Making Decisions and Rules</td>
</tr>
<tr>
<td>G.2.5</td>
<td>What conflicts of interest could arise and what is the approach to addressing? In which cases would the Solution use the noted mechanism for disqualification of members in official matters vs when that conflict would be waived (the two examples cited on pg 164 of the proposal)?</td>
<td>Managing Conflicts of Interest</td>
</tr>
</tbody>
</table>
Faster Payments QIAT

DRAFT ASSESSMENT
Faster Payments QIAT

DRAFT ASSESSMENT

Proposer: WingCash

Summary Description of Solution:

The WingCash solution, known as the Faster Payments Network (FPN), is a software platform that, as proposed, would be owned and operated by the Federal Reserve and the Governing Organization (GO). The proposer recommends the GO be comprised of members of the Faster Payments and Secure Payments Task Forces.

The FPN uses a digital currency for payment. This currency, called “digital Fed notes,” would be issued by the Federal Reserve and is tied to the Federal Reserve Bank’s Internet domain (e.g., fednotes.com). The Federal Reserve would control the digital Fed notes, but authenticated individuals and businesses would be able to hold, transfer possession of, and deposit these notes. The end-to-end payment process begins with a person or business completing a one-time enrollment in the FPN, then continues through the iterative steps of authentication, payment order, receipt, and optional reconciliation (upon conversion or redemption of Fed notes in U.S. dollars or other currency). Changes in possession on the FPN occur directly between payer and payee without transfer fees.

Each digital Fed note is a unique webpage with an unchangeable URL (e.g., fednotes.com/usd/ml14060622c) with a single, permanent monetary value. In addition to the URL, each Fed note is assigned a single, permanent, monetary unit of value (e.g., $0.01 to $100). Because these notes are similar to cash, they could be used as cyber-currency or stored in digital wallets. Fednotes.com would publish the digital Fed notes, each of which includes the issuer’s URL and the current holder’s URL, which is a pointer to the holder’s profile unless masked for privacy reasons. The FPN is thus a system of payment addresses (the URLs), not accounts. Payments would be conducted by changing the possession of each Fed note—i.e., changing the owner of the URL. The URLs mapped to a payment address or payment address alias such as an account at a depository institution would be stored in the “Global Directory Service” (GDS).

The technical design of the FPN allows for closed-loop value issued by a businesses in standard denominations. The proposal refers to this as “brand cash.” Brand cash is restricted as determined by the issuer and FPN rules and the digital note includes the issuer (e.g., the business name), the redemption locations, the holder and other information.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths

– A digital currency solution that increases accessibility by enabling all end users (individuals acting on their own behalf or on behalf of a business) to enroll directly through the FPN enrollment page (e.g., fednotes.net/signup), essentially creating user payment addresses in a ledger directly with the Federal Reserve
- Features such as brand cash for closed-loop currency; payment codes that allows the payee to require the payer to present a unique payment code to the payee for validation before the transfer can be complete; and the ability to customize individual payment address and share it publicly on social media can all increase adoption and allow the solution to be used across a range of use cases, including POS.

- High degree of usability and predictability based on the videos of end user experience shared in the proposal.

- Provides real-time funds availability and immediate settlement through digital notes, minimizing credit and liquidity risk. It is designed and engineered to prevent fraud and minimize user errors. No Personally Identifiable Information (PII) is handled or exchanged, further mitigating risk.

**Areas for improvement and enhancement**

- The solution hinges on the willingness of the Federal Reserve to own and operate the FPN (and create new monetary policy). Adoption has challenges unless Fed notes are legal tender, since depository institutions would give up revenue associated with current payment systems and other new security and technical infrastructure would need to be built.

- A few models for distribution of Fed notes are described – bank-centric (Fed issues digital notes to banks who would redistribute digital notes to individuals. Proposal intends for identity verification associated with payment addresses to be the responsibility of the GO rather than the bank), bank-light (Fed is responsible for validation of the identity of payers and payees), or a hybrid (multiple tiers of transaction authorization based on level of identity validation). In the bank-centric model, providers especially need to have enough motivation or incentive to adopt the solution and make it available to end users. In addition, having the GO responsible for identity verification of all users creates significant new build and execution challenge.

- The solution requires the capacity to issue and hold billions of web addresses, creating a security and scalability challenge for the Federal Reserve and GO to jointly manage.

**Use cases addressed**

- FPN addresses all domestic and cross-border use cases, including B2B (business to business), B2P (business to person), P2B (person to business), and P2P (person to person). It also covers closed-loop notes.

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

- The solution has already been deployed on a smaller scale. It has a proven track record and provides videos that demonstrate the user experience. However, the solution is dependent on Central Bank adoption to issue digital fiat currency and be the operator, as well as regulatory changes.
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 Fast Payment Network (FPN) is easily accessible to all U.S. consumers and businesses (U.1.1). It does not require a bank account (U.1.4); users directly enroll and need only to provide basic personal information (e.g., name and address) and to choose their authentication approach—such as a password, a hardware key, or a biometric token. Anyone can establish a unique identity and token. In addition, any recipient can receive a payment (U.1.2); if a recipient is not enrolled in the solution, he/she receives an invitation with instructions to enroll before receiving the payment. Users can also transfer or deposit their Fed notes to checking or savings accounts at depository financial institutions. The FPN supports multi-currency by having other Central Banks or financial institutions issue national currencies to the GDS (U.1.3).

The solution’s plan for achieving widespread adoption relies on the Fed to operate and issue Fed notes as legal tender, to gain the trust of individuals and entities using the FPN, and to assure overall public confidence. The implementation plan includes achieving commitments from top retailers (who can issue closed loop value, utilize branding opportunities in FPN) and depository institutions (motivated by branding opportunities, reduction in costs, and a potential fee for distribution or deposit of Fed notes) (U.1.5).

While end users often use physical cash for its anonymity, anonymous transfers are not possible in the FPN which could create adoption challenges. The FPN does, however, enable privacy for transfers (e.g., each Fed note, under the rules, may not be required to publicly show the end user’s identity). The solution plans to achieve end user adoption of digital currency through a value proposition around accessibility and ease-of-use, free transfers, ability to hold and redeem closed loop value, the personalization and social media aspects (ability to share payment addresses) and the public trust in the Federal Reserve.

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 demonstrates a straightforward, simple end-user experience (U.2.4) that is available 24x7x365 through email, phone, a social media address, or the payee’s primary payment address in the directory—as long as the user has a device and an Internet connection (U.2.1, U.2.3). To enroll, users need only to provide basic personal information (e.g., name and address); they are then assigned a unique identity and token with which to make payments (U.2.2). The FPN technical design enables initiation of payments through email, phone number, social media address, primary payment address of a payee, or custom payment address of a payee in the GDS, a widget on a website or published application. The solution’s design accommodates varying levels of technological proficiency and addresses the needs of individuals with disabilities, the elderly, and those with limited English proficiency (U.2.4). In addition, payment status is transparent to users at every step of the transaction (U.2.3).
U.3 Predictability

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The FPN clearly defines its baseline features, which are delivered consistently and centrally by the Federal Reserve and the FPN’s Governing Organization (GO) (U.3.1, U.3.4) and comply with the relevant laws (U.3.2). The solution communicates transactions’ costs and implications to end-users before the transaction occurs (U.3.2), as demonstrated by the proposal’s visuals. The solution employs Internet standard communication and messaging protocols (U.3.3), but allows providers to customize their user interfaces. Finally, it clearly defines error resolution protections, rights, and liabilities and makes those easy for payees to understand (U.3.5), as well as mechanisms to reduce the incidence of unintended payments (e.g., message prompts to the payer to confirm payment to a new recipient). Several generic terms are provided to distinguish the solution from other payment methods such as digital banknotes and Fed notes (U.3.6).

U.4 Contextual data capability

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale**
The FPN supports contextual data including data fields identified on pg 79 of the proposal (U.4.1). It indicates that the Fed and Governing organization will determine the actual message formats and data dictionaries to be supported at implementation. While the default message format of the FPN is JSON, the technical design provides data translation to other standard message formats including ISO20022. The FPN enables easy integration with business and personal finance systems by enabling end users to apply tags to transfers and define data dictionaries for automated use with external systems (U.4.2). The solution balances the need for flexibility with the need for standards by allowing both unstructured and structured formats, and supporting data fields in a custom defined data dictionary as well as the ISO20022 standard (U.4.3).

More detail would be helpful on the ability of JSON to support the contextual data requirements of corporate (B2B) payments. Given the dependence on translation, the Proposal needs to ensure that the translation engine is 100% effective and doesn't lead to errors or omissions.

U.5 Cross-border functionality

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

**Rationale:**
The FPN enables cross-border payments through its technical design that allows rules, regulations and laws to be incorporated into the network logic (U.5.1). Interoperability with other Payment can only be achieved by adopting the FPN and implementing the necessary code changes to support another network’s rules and regulations (U.5.2). The FPN ensures that providers disclose exchange rates and fees to the payer (U.5.3) and allows for conversion from one currency to another by
alloying the payer to determine the currency to transfer and allowing the payee to convert the currency as desired through conversion exchange providers (U.5.4).

More detail would be helpful on how the FPN is compatible with other networks (such as ACH, card networks Dwolla, Ripple) as noted on pg 81 (U.5.2). The implementation plan for cross-border is rooted in confidence that if the U.S. adopts digital currency, other countries will follow, but further detail would be helpful on any go-to-market plan for other countries issuing national currency as part of the GDS (U.5.5).

U.6 Applicability to multiple use cases

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

Rationale:
The FPN covers all use cases for both domestic and cross-border payments. Its target use case centers on P2P payments; many of the concepts and details of this use case can be extended to other cases as well. The solution would be enhanced with more detail on its applicability to corporate (B2B) payments.

Efficiency

E.1 Enables competition

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

Rationale:
Because FPN transfers are free, the competition between providers is based on offering superior user experiences and value-added services that extend the baseline features using the GDS and the API (E.1.1). End-users can choose whichever provider they prefer and use multiple integrator applications at the same time but spend Fed notes only once. Switching integrators just requires opening another application since the value of Fed notes for the end user displayed in any mobile application is updated in real time to reflect transfers made by the end user (E.1.2). Any provider with a feasible application that can integrate through the FPN’s API can participate (E.1.4). In addition, the solution requires providers to disclose total costs to end-users in advance and provides strong examples of this capability (pages 85-86) (E.1.3).

E.2 Capability to enable value-added services

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

Rationale:
The solution allows any provider or “integrator” to provide value-added services through the use of an open API (E.2.1). Potential value-added services might include products such as “branded cash” (e.g., bank-branded frequent flyer miles). All providers meeting the participation requirements can
be integrators and develop customer interfaces, software applications, mobile applications, and services (E.2.2). The FPN requires providers to clearly disclose to customers that the value-added services are optional (E.2.3).

E.3 Implementation timeline

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

Rationale:
The solution has a track record, having operated with fully developed and market-tested features in other markets since 2011.

The FPN’s implementation plan includes a plan for funding (describing both the funding required by the Federal Reserve and Governing Organization and how to recoup it through cost reduction associated with physical cash), implementation and ubiquity hurdles and plans to overcome those hurdles, entities targeted for first adoption of the solution (top retailers, providers), market share and growth projections and projected timeline compared to historical examples (E.3.1). The solution acknowledges that achieving ubiquity for a payment service by 2020 is unparalleled in recent history.

The implementation plan is heavily dependent on three things: 1) the Federal Reserve commitment to owning and operating the FPN, as well as a Governing Organization that is capable of securely validating all users of the FPN, 2) the adoption by businesses, billers, merchants to enroll in FPN, integrate at the POS, and issue closed loop currency as an incentive for customers who pay using the FPN, and 3) the participation of providers as a distribution mechanism to customers that have a payment address linked to their account with the depository institution. In terms of incentives, the proposal mentions that banks can charge end-users a fee for distributing or transferring the FPN to their deposit/credit card accounts, but this is likely to be weighed against revenue streams from the system today.

E.4 Payment format standards

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

Rationale:
The FPN’s standard message format, Javascript Object Notation (JSON), can interoperate with existing payment format standards through data translation (E.4.1). Given the dependence on translation, the Proposal needs to ensure that the translation engine is 100% effective and doesn't lead to errors or omissions. The solution addresses cost-effectiveness of the message format by allowing integrators to choose their message format (E.4.3) and addresses a mechanism for updates by allowing for choice of standard message formats to be supported through data translations to/from JSON (E.4.4). The solution uses message formats published by recognized standards development organizations (E.4.5).
E.5 Comprehensive

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The FPN's solution is comprehensive, with simplifying approaches to traditionally cumbersome stages. It enables all aspects of the end-to-end payment process, performing receipt, clearing, and settlement simultaneously (E.5.1). Its technical design supports all of its features, including its usability, reliability, performance, information security protocols, operations, compliance controls, and risk controls (E.5.2).

E.6 Scalability and adaptability

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The FPN technical design supports projected use cases (E.6.1) and is based on web-based, open standards. The technical design is adaptable given it is based on Internet and open standards and provides an API for integrators that can be used to address changing technological and customer-driven demands. In addition, the Federal Reserve controls the solution through a single, universally trusted and authoritative Internet domain and can drive the response to economic and regulatory developments (E.6.3).

The solution today can reach a capacity of 23 billion transfers per year, but the proposers believe with hardware and software optimizations, the FPN can handle 220+ billion transfers per year (E.6.2). The solution uses distributed architecture that spreads the storage and query load among many databases; however, the scalability required for implementation is unprecedented.

E.7 Exceptions and investigations process

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The solution provides an application layer protocol that allows changes in status of all network applications to be monitored in real-time. In addition there is an administrative tool to identify and resolve transfer errors, failed sign up attempts, cancelled payment addresses and other exceptions (E.7.1). The solution ensures information is created, recorded and retained or a period of time specified by the operating rules – information relevant to every transfer is captured and stored (E.7.2). Exceptions data and transfer errors are captured in a centralized logging repository. The FPN will use these logs to spot exceptions not visible to the individual participant (E.7.3). The fraud protection group within the FPN will analyze exceptions, determine and develop the right response for handling.

More clarity on the protocols for addressing exceptions in a reasonable timeframe would be helpful (E.7.1).
Safety and Security

S.1 Risk management

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

**Rationale:**

FPN’s risk management framework outlines the roles and responsibilities of the Federal Reserve and notes that the architectural design of FPN is adaptable to law or regulation (S.1.). (S.1.1). The solution’s settlement approach mitigates risk because Fed notes act like cash, and no intermediary FIs need to transfer the money (S.1.2). The solution addresses measures to prevent and reduce the risk of unauthorized, fraudulent, and erroneous payments (S.1.4). For instance, payers must sign and reconfirm push payments at the time of payment because the payment is irrevocable once it is executed. Since payments occur directly between payers and payees through the FPN, special incentives are not needed for Providers to contain risks they pose to other Participants (S.1.5). The Governing Organization will ensure the FPN’s risk management framework is subject to periodic review (S.1.6).

However, several descriptions of the risk management framework are still high-level, in particular, more details are needed on how the FPN addresses operational risks (S.1.3).

S.2 Payer authorization

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

**Rationale:**

Because the FPN uses Fed notes, payers do not need to obtain authorization from their depository institution whenever they initiate a payment; instead, payers can directly pay payees without their depository institution’s acting as an intermediary (S.2.1). The solution allows payers to pre-authorize payments using payment codes, but this “pre-authorization” is not pre-authorization for a payment on a future date as that capability is not currently available (S.2.2, S.2.3).

S.3 Payment finality

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

**Rationale:**

Because users pay with digital Fed notes, which guarantee good funds, no depository institution needs to approve their payments (S.3.1). The transfer is irrevocable when the FPN displays the confirmation page after the payment order has been executed (S.3.2). The FPN transfers the value before notifying the payer and payee.

The design principles of the FPN are intended to mitigate the need for an intermediary to resolve disputed payments. The proposal indicates that the FPN will have rules and regulations to protect payers and resolve disputes, but more detail is needed on the mechanisms and processes to protect or compensate the payer in cases of disputes (S.3.3).
S.4 Settlemen approach

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

**Rationale:**

The solution settles payments in central bank money (i.e., digital Fed notes) (S.4.3). FPN’s transfers of the Fed notes do not incur settlement obligations between a depository institution and/or a Regulated Non-Bank Account Provider because the payments are sent directly from payer to payee (S.4.1). As a result, there is no inter-provider liquidity risk (S.4.2).

S.5 Handling disputed payments

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

**Rationale:**

FPN’s approach focuses on best practice processes and procedures to reduce errors and prevent fraud. In terms of handling disputed payments, its rules clearly state that the payer is accountable and financially responsible for all incorrect or erroneous payments (S.5.1). The solution does not include a consumer payer’s provider in the transfer of Fed notes (S.5.2). The payer and the payee can request a return of the funds, but the outcome depends entirely on the payee’s consent (S.5.3). The FPN approach to protecting business, government and consumer payers from losses related to fraud or errors is to implement processes that reduce the chance of errors and fraud. Liability allocation when fraud or error does occur, however, is on the payer (S.5.5).

The design principles of the FPN are intended to mitigate the need for an intermediary to resolve disputed payments. The proposal indicates that the FPN will have rules and regulations to protect payers and resolve disputes, but more detail is needed on the mechanisms and processes for dispute resolution within the FPN (S.5.1).

S.6 Fraud information-sharing

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

**Rationale:**

The FPN streamlines the process of information sharing by centrally collecting and aggregating information for all transfers under the Internet domain where the Fed notes are issued (S.6.1, S.6.6). The sharing mechanisms are based on standard data interchange formats and protocols and include activity feeds available to participants and integrators (S.6.4). These sharing mechanisms enable real-time updates and alerts to participants (S.6.3). The FPN continuously logs, reviews, and monitors data about participants (individuals, businesses, and financial institutions), which enables the FPN to identify and evaluate potential risk patterns in real-time system-wide (S.6.7). The solution then uses data analyses to determine and act on mitigating strategies. It employs a roles-based permission system to control data sharing (S.6.5).
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 FPN has layered, robust technical, access, operational, procedural, and managerial controls that address and foster security (S.7.1-3). These controls help protect and maintain the integrity of confidential, private, and sensitive data (S.7.1). Security controls are especially strong where the Federal Reserve and Governing Organization are responsible for policies, controls, and oversight. These strengths are particularly important for protecting the application layer, which will face continuing and intensifying security threats.

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 solution defines its target metrics and approach, referring to FPN’s availability as “five nines”—i.e., 99.99% (S.8.1). The solution ensures those target availability metrics can be achieved through excess capacity, mechanisms and technology to deal with DDoS attacks and other types of cyber-attacks. The implementation team will also develop and implement comprehensive business continuity and disaster recovery policy (S.8.2). The Governing Organization will ensure sufficient resources are devoted to business continuity and resiliency and will also oversee the contingency planning process (S.8.5). The solution has the Federal Reserve acting as the redeemer of last resort to minimize the chance that adverse FPN-related events will cause other market participants to fail to meet their obligations (S.8.3).

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 solution’s Global Directory Service (GDS) protects sensitive information and eliminates the need for payers and payees to exchange depository account information (S.9.1-3). The GDS stores all Personally Identifiable Information (PII), which is then replaced by URLs—electronic addresses that link to payment card and account information but do not store it. These are exchanged in the messages and used to process payments. All the URLs are tied to the Federal Reserve’s web domain and become invalid if someone tries to use them outside this domain.
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 FPN requires robust identification and verification when enrolling and interacting with end-users and providers. It supports authentication methods that include identify service providers, passwords set by end users, PIN and devices with cryptographic keys and biometrics identification (S.10.1). In addition the GDS, payment codes and ability to conduct test transfers ensures the payment is destined to reach the intended payee (S.10.2). FPN aligns with regulatory guidance and industry standards for authentication (page 128) (S.10.3).

The FPN also applies strong end-user authentication controls across all delivery channels and can vary the authentication procedure based on the risk-weighting of a given transaction (S.10.4-5). The API adheres to OAuth2. End user authentication requirements can be based on an individual’s permissions in the FPN. The Governing Organization is responsible for ensuring the FPN adopt new and decommissions old authentication models based on the evolving threat landscape (S.10.6).

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 solution outlines the agreement for providers that choose to participate in the FPN including requirements around deposits, information systems, regulatory and legal requirements (S.11.1).

The FPN does not require special participant requirements for depository institutions but utilizes the existing regulatory regime. The only change needed for depository institutions is the responsibilities and requirements associated with distributing Fed notes (S.11.2).

The FPN Governing Organization will regularly monitor and ensure compliance with the participation requirements. In addition, the FPN will implement participation requirements in the software code as much as possible (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:**

Because payments are executed by transferring ownership of Fed Notes via their URL, they do not require the approval of the payer’s depository institution or regulated non-bank provider. This satisfies the Task Force’s “Very Effective” criterion of executing approval within two seconds. Good funds are assured because Fed Notes are considered legal tender issued by the Federal Reserve.
F.2 Fast clearing

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The FPN requires the payer and payee to exchange payment information in real-time without the need for a depository institution or Regulated Non-bank Account Provider to exchange payment information. This satisfies the Task Force’s “Very Effective” criterion of clearing within two seconds.

F.3 Fast availability of good funds to payee

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The FPN executes all submitted payment orders in real-time and immediately displays a confirmation page to the payer indicating that the transfer is complete. The payee can withdraw or transfer these funds immediately. This satisfies the Task Force’s “Very Effective” criterion of availability of good funds within one minute.

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

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
This satisfies the Task Force’s “Very Effective” criterion of settlement within 30 minutes because there is no lag in settlement with FPN transactions and no credit or liquidity risk for providers (F.4.1). Transactions are settled immediately upon payment confirmation (when possession of the digital Fed note is transferred from the payer to the payee), which occurs 24x7x365 (F.4.1). There is no lag when settling across different time zones (F.4.2). The FPN also allows payers to specify a later time for payment execution and will thus defer the payment, but the payment will still settle immediately at that later time (F.4.3).

F.5 Prompt visibility of payment status

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

**Rationale:**
This satisfies the Task Force’s “Very Effective” criterion of visibility within five seconds because both the payee and the payer are notified immediately when possession of the digital Fed notes changes (F.5.1-2). Once the FPN changes the possession of the Fed notes, it sends a confirmation of successful payment to the payer and the payee. The payee has good funds in digital Fed notes the moment those notes’ possession changes. If the FPN cannot change possession of the notes from
the payer to the payee, it immediately sends an error message to the payer to notify them in real
time that the transfer did not succeed.

Legal

L.1 Legal framework

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

**Rationale:**
The proposal articulates a thorough legal framework for managing digital Fed notes and delineates the applicable laws and the necessary changes that would be required (pages 137-141) (L.1.1). FPN has conducted several rigorous assessments of the framework and provides an extensive description of the legal sources, potential gaps in those sources, plans to close those gaps, and the means by which it will support compliance (pages 146-151) (L.1.1-2, L.1.4). As part of this description, the proposal addresses potential revisions that might be necessary to the Federal Reserve Act and offers thoughts on those revisions (pages 142-144). The proposal also explains how entities and payments through the payment system (from payer to payee) will be legally bound within the proposed legal framework for the solution (L.1.3).

L.2 Payment system rules

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

**Rationale:**
The FPN has requirements, standards/protocols, and procedures that govern the rights and obligations of all end-users, providers, payers, and payees. The solution’s payment system rules cover all required features of L.2, including providing an error resolution process for end-users (users are accountable and financially responsible for errors on signed and executed payment orders while the Governing Organization has responsibility to resolve system errors) (L.2.5) and allocating legal responsibility to the appropriate entities to obtain valid authorization for payers (the rules permit only the payer using valid credentials and acting on its own behalf to sign and submit an order to the payment system) (L.2.4).

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:**
FPN has a legal framework and procedures that allocate legal and financial responsibility for losses in the event of a payer or payee claim of disputed consumer payments (L.3.1). It also provides options where it, end-users, and providers can establish additional consumer protections for payments (L.3.3).
The FPN is designed with strong protections to prevent fraud and errors. However, more clarity is needed on the support the solution provides for resolution of consumer claims arising from errors that do happen (L.3.2).

**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 Governing Organization will establish and adhere to a privacy policy for the payment system which will include when and how payment and related information can be collected and disclosed so that it is consistent with applicable policies, laws, and end-user preferences (L.4.1). The solution describes its approach to data security of payment and related data including legal requirements, and various protections in place through the system (L.4.2). The nature and type of end-user data that may be required for security, legal compliance, and authentication purposes within the solution are described (L.4.3). End-users have visibility into the data collected on them and some control over the data being collected (L.4.4). The proposal is also clear about the responsibilities for data breaches at FPN, at the end-user, or at a provider (L.4.5). The Governing Organization is responsible to protect against data breaches and threats. For instance, end-users are accountable and financially responsible for losses associated with the misuse or theft of their credentials.

**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 offers an open-source version of the current embodiment of the FPN available at wingcash.org. On January 2011, the inventor conducted an international patent search for claims – the holder of the patents is willing to license or transfer the patent to the Federal Reserve or the Governing Organization under mutually acceptable terms. The FPN’s open source application stack can be replaced with equivalent proprietary applications from other vendors to achieve the faster payment capabilities of the proposed solution.

**Governance**

**G.1 Effective governance**

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

**Rationale:**

The proposal lays out governance arrangements that ensure efficient decision- and rule-making (G.1.1) and that provide a clear appeals process (G.1.3). These arrangements are publicly disclosed.
(G.1.2) and provide for independent validation of compliance with FPN’s rules, applicable laws, and achievement of relevant objectives (G.1.4).

G.2 Inclusive governance

**Rationale:**

The solution’s process for implementing new rules includes a commentary period from the public. In addition the rule making committee is required to publish how public comment was addressed in the rulemaking process (G.2.1). The Governing Organization of FPN has a diverse composition, and the FPN provides all stakeholders with a chance for input and influence (G.2.2). The Governing Organization will create advisory bodies, including one for financial institutions given their role as distributors of Fed notes (G.2.3). FPN’s governance approach enables specific stakeholders or stakeholder groups to proportionately influence outcomes through representation within these governance and advisory groups (G.2.4). The solution addresses and manages actual, perceived, and potential conflicts of interest by establishing processes and methods to identify, disclose, and manage conflicts of interest – one mechanisms would include disqualifying members of the Board, executive team or staff members from participation in official matters (G.2.5).
# APPENDIX A: ASSESSMENT SUMMARY

**UBIQUITY**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>QIAT Assessment</th>
<th>Proposer Self-Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.1: Accessibility</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>U.2: Usability</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>U.3: Predictability</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>U.4: Contextual data capability</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>U.5: Cross-border functionality</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>U.6: Multiple use case applicability</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**EFFICIENCY**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>QIAT Assessment</th>
<th>Proposer Self-Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1: Enables competition</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>E.2: Capability to add value-added services</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>E.3: Implementation timeline</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>E.4: Payment format standards</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>E.5: Comprehensive</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>E.6: Scalability and adaptability</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>E.7: Exceptions and investigations process</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**SAFETY AND SECURITY**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>QIAT Assessment</th>
<th>Proposer Self-Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SAFETY AND SECURITY (cont’d)</td>
<td>= QIAT Assessment</td>
<td>○ = Proposer Self-Assessment</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>SPEED (FAST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.1: Fast approval</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>LEGAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.1: Legal framework</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>○ ✓</td>
<td></td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>GOVERNANCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G.1: Effective governance</td>
<td>✓ ○</td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td>✓ ○</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

Assessors, we appreciate your work evaluating this proposal. Thank you for your efforts.
WINGCASH PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

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

The proposal requires significant Federal Reserve engagement –to own and operate the software platform. This scenario is not viable at this time and the solution should not be assessed against the effectiveness criteria. If we want to rate the solution, it should be characterized as an academic exercise at this point in time.

While overall I somewhat agree with the assessment, I don’t agree with some of the individual assessment criteria ratings, primarily because of the rather massive assumptions on which the solution is reliant. For example, given the rather large and time consuming issues associated with the underlying assumption of creating a new currency and associated infrastructure, I believe effective for items such as implementation timeline are unrealistic. Similarly, rating Scalability & Adaptability as very effective given the massive scope of the implementation seems a bit overreaching. If I am reading the proposal correctly, the solution also makes assumptions that there would be no cost for services that would be provided by other entities (e.g. Federal Reserve). How will those services be funded if no fee?

While I commend WingCash for getting outside the box in their proposal, I question the number of Very Effective ratings given the big shift in the role of the Federal Reserve as essentially they will be holding accounts for end-users. How are the following issues addressed by the Federal Reserve: BSA/AML/KYC issues at time of enrollment and with ongoing activity, dispute resolution, customer support as everything cannot be resolved online as evidenced by the existence of call centers in FIs and businesses, and suspicious activity monitoring as relying on strong authentication is not taking a layered approach to fraud mitigation. Before all this is the consideration that would have to be given by Congress and the taxpayers to essentially have the Federal Reserve act as an end-user provider of financial services competing with the free market. Again I think WingCash has brought forward an excellent proposal, but I feel the assessment does not accurately assess the challenges associated with implementing said solution. Great work WingCash stretching our minds.

Innovative and interesting concept – the Fed would stop issuing paper currency and only issue digital currency called Digital Fed Notes. But not sure how their model FPN, with the Fed Notes and their unique connection to a single Internet domain, which would be under the control of the Fed, will benefit Faster Payments.

Wing Cash is a software platform called Faster Payments Network (FPN), with combined ownership & operator of the Federal Reserve (Fed) and Governing Organization (GO). FPN model to have ownership of public and private, with specific roles for Fed, Department of Treasury and extension of Fed Cash Service. While an interesting concept, it would require extensive proof-of-concept testing before widespread adoption would be considered.

Although I thought this was a good solution as it was unique, I do believe the ratings were too high.
Cutting-edge technology that very nicely addresses the unbanked. Ideally, dependent on central bank is operator/issuer. The solution is such a paradigm shift it may hinder adoption. It would appear that cash out would be another impediment.

E.3: Implementation Timeline: This should be very effective, not merely effective. The solution has already been implemented in the United States. It is not necessary to invent new technologies; there is no need for an extensive roll-out by third-party suppliers (i.e. retail-facing outlets), and it allows for remuneration by market entrants.

S.3. Payment Finality: This should be considered "very effective," instead of "effective." In the case of the Fed-lite proposal, the use of banks as intermediaries in transactions should confer the ability to contest payments. That system safeguards a settlement process inside the Fed that would be verifiable through entirely authenticated good funds accounts.

S.3.3 Contested Payments: Should be rated as "somewhat effective." The system does not provide a means to contest a disputed payment after execution of the payer’s digitally signed order.

S.5: Handling disputed payments: It should not be considered effective, but at best, somewhat effective and perhaps not effective. The system relies upon the voluntary return of funds by the payment recipient. As acknowledged by the proposer, the solution does not prevent fraud by inducement. The proposal only suggests that the FPN should develop a system for rules and regulations to govern disputes.

U.4. Contextual data capability should be "very effective," rather than "effective." A full unique URL can provide extensive information. It is hard to imagine a more complete solution for messaging.

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 provide the capability for a future dated pre-authorization. The solution returns funds at the payee’s consent only. The solution’s disaster recovery and business continuity policies are not written. The solution is only applicable if the Fed agrees to own and operate the solution and create a new monetary policy.
Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

Safety assessment rating off the mark from criteria expectations. Acceptable that solution pushes most secure validations onto financial institution, but there is a lack of security proof within their product. Governance rating also too high based on the solution’s total lack of governance.

Assumes the Federal Reserve will issue and control a new currency, called "digital Fed notes."

1 - Digital currency, 2 - Increases accessibility, 3 - Unique payment codes for transfers to be completed are required, 4 - Provides real-time funds and availability, 5 - Has been deployed on a smaller scale, 6 - Fraud information sharing seems highly effective, 6 – speed of 2 seconds

The WingCash proposal was extremely well done and addressed all of the Effectiveness Criteria. This cannot be said for some of the other proposals submitted and reviewed by this reader. It was clear that considerable thought, time and effort went to producing this proposal.

While the proposal represents a departure from the more traditional payment processing practices it clearly defines the features, benefits, roles and responsibilities needed for a new operating model and the introduction of this new method of payment (real-time payments).

Liked the digital FED Notes medium as a way for the FED to control and manage the digital money supply. Closed-loop branded digital cash supports high degree of usability and predictability. Real-time funds minimize credit and liquidity.

Interesting concept of creating billions of unique web addresses—FED Notes. Requires the Central Bank’s participation. Question about how to secure and protect the ownership of records?

One of the best proposal presentations of the group of proposers. In the realm of faster, digital payments would appear to have great potential.

Comparatively, the payment format standards seem too highly rated compared to other solutions that also had proprietary standards that required translation to another standard.

In my agreement I focus on the central problem with respect to positive evaluation of the proposed solution: "... the solution is dependent on the Central Bank adoption to issue digital fiat currency and be the operator, as well as regulatory changes." If The Fed had interest in a centralized, authoritative payments system, it would have created one already. Simply because technology aids the possibility does not change the political environment in which The Fed exists and its overall structure.

I like proposals that include the FRB as a key part of the solution. Wingcash includes an active FRB involvement.

I struggled with this proposal’s assessment. The proposal was extremely well done. Reading the proposal at face value, I think the ratings are somewhat reasonable. However, the proposal focuses on
a solution that relies 100 percent on the Federal Reserve. I am just not sure this happening. I like how the proposal addresses legal and governance framework and I like the idea of the FPTF and SPTF serving as a governing organization.

The ratings were a bit generous.

Overall, I think it was fine but I had a concern with the S.7 result of Highly Effective. The solution by default provides for single factor authentication but supports multifactor. This seems to warrant an “Effective” S.7 value?

**TASK FORCE SOLUTION-ENRICHING COMMENTS**

**Ubiquity**

Reliance on US Payment Systems to embrace digital currency in order to have the solution available to all end-users through the established FPN. Limitations with only members of the FPN can lead to not all payment users adopting this option.

Thank you for this submission, the concept of digital currency is a unique solution for faster payments. Government involvement in transactions of commerce however may be overstepping and uncomfortable to citizenry.

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. This removes financial institutions from the equation as they would sign up with the FPN individually. I think I would like to a way that users sign up for the FPN through their financial institution.

The solution could be enriched by providing the progress, if any, of obtaining the willingness of the Federal Reserve Bank to own/operate the Faster Payments Network (FPN) and to create a new monetary policy for the usage of digital currency (Fed Notes) for payments.

Describe how contextual data will be defined, agreed to and understood by not only the entity or person sending the data, but also the receiving party in a way that can be anticipated before receipt.

The proposal could be enhanced by the use of a non-governmental, central authority for the needs of the proposal. That could be in the form of a single, or collection of banking entities to facilitate the needs of the proposal currently envisioned as The Fed by the proposer.

Solution relies on Federal Reserve and so far they have stated they do not plan to participate or serve in this capacity.

Federal Reserve has to be willing to do this, proposed Governing Organization has to be willing to do this. Adoption by businesses and merchants adds to timeline – if the Federal Reserve was on board then it may incent the businesses and merchants or it may have the opposite effect.
Feasibility/viability may hinge on the FRB’s willingness to operate the FPN.

The Postal Service is an untapped resource for the distribution and utilization of a faster payment system. The proposal provides some interesting ideas here. The proposal could be improved by sharing additional thoughts on how the Federal Reserve, US Postal Service, and US Treasury would collaborate on an initiative.

The proposal offers a detailed glimpse at what an API-first payment system might look like and how developers could interface with and build on top of it. Great contribution to the task force process.

The proposal could be improved by sharing more information on how the FPN complements DI OFAC obligations associated with digital transactions.

The preference of more modern standards and languages over ISO 20022 should not preclude or marginalize the proposal in any way. The payment industry would do well to embrace more modern paradigms that are more in line with the needs and expectations of the 21st century (i.e. JSON > XML).

With that said, tapping ISO 20022 messaging for network/infrastructure and placing translation services at the fringe could be a good compromise.

State and federal governments have different financial, technical, and regulatory requirements for payment systems and services (e.g., The US Treasury’s Green Book on ACH). The proposal would be improved if it discussed how the FPN has or would operate with government agencies.

Appears that this solution relies on the FED to distribute the technology to participating financial institutions and trickle down the technology into the market. Would recommend finding a different channel to distribute to the market.

Assumes users will in effect have accounts with the Federal Reserve. Fed has not built the infrastructure (accounting, account statements, dispute support, customer support, BSA, etc.) to contemplate such a role. Understand this is conceptual but would take a significant investment requiring support from Congress, private sector, and taxpayers. Feels like a tall order in today's environment.

As the voice for all stakeholders within the ATM industry, ATMIA believes that ubiquity is a very important aspect of any new faster payments system. The ATM channel serves as a means to connect physical cash to electronic cash and all other forms of electronic payments. WingCash is a very interesting approach to doing so and would seem to offer flexible and effective solutions that could be utilized by a broad range of consumers.

ATMIA does have some concerns over the potential for a registration process to create obstacles for consumers—particularly the unbanked and underbanked, who rely heavily on the ATM channel for their financial services needs. The registration process described here, however, does seem to be quite simple and offers options for at least some level of anonymity. It should be kept in mind, as well, that the use of cash requires no registration process whatsoever—so the least burden possible is highly desirable.
U.6 – Use cases. We like the concept and possible applicability for B2B payments. As the main use case seems to be P2B at POS, wondering how practical the solution is for B2B payments?

Ubiquity for WingCash is doubtful. This is due to two types of inhibitors: things the system doesn't have a clear or good answer for and things that are likely to be unappealing to other systems who it would be assumed would have to connect to WingCash to enable ubiquity to be achieved; or things that are both unclear and likely to not be desired by other players. The scheme didn't seem to have clear answers regarding: How a bearer-based instrument would be efficiently conveyed to another party; the assumption that the Fed would offer the scheme (and what happens if the Fed doesn't want to or can't); the concept of the scheme being a public utility is unclear and seems to conflict both with the idea that the Fed would run it and with the scheme having no revenue. They seem to not have adequate answers for how the scheme would cover its costs since they say it will have no enrollment fee, no account fee and no transaction fee. Interoperability with other schemes is asserted, but not explained adequately but interoperability between schemes that have costs and prices and a scheme that has no pricing would be difficult if not impossible to negotiate.

Efficiency

Potential issue with the network capacity for the number of transfers that can be done within a year and how this may impact users’ ability to offer this solution. Expectations of hardware and software optimization for larger capacity appear untested at this time.

Not sure it is possible with the reliance on the FED, but to the extent the system could work outside the FED would be valuable information to consider.

Scalability issues related to holding billions of web pages.

How would banks’ core payment processors feel about this solution? It would impact their revenue streams.

Can impact banks’ revenue streams related to current payment methods, even if banks were able to charge an end-user fee.

The proposal places a heavy burden for acquisition on a wide range of key stakeholders. While this is true of nearly every proposal in the process, the uniqueness and novelty of this solution does create a higher bar for it to jump over.

The proposal’s timeline is pretty aggressive in both its start date and expected progress (e.g., calls for a Q1 2017 timetable for adoption of this proposal and finalization of its GO charter). If this is feasible, the proposer should provide additional details on this would be achieved. If not, proposers may want to shift the start date to accurately reflect a more achievable timeline.
Its incorporation of domain name aliasing offers FIs an incredibly accessible and pragmatic way to offer the FPN to their system. The proposal could improve its submission on discussing how FIs’ core service providers would help enable this, and other sorts of functionality and experience.

While the Fed (a public/private institution) has a fiduciary obligation to reduce costs (as noted in the submission), it is also legally required to operate at-cost (or close as possible). Merely saving money will not sustain an operation of this magnitude or justify its existence after an ROI is claimed. As a public/private entity, the Fed may find securing the funding a solution of this size difficult (may also require additional congressional approval?). The proposal could be improved with additional information on how the proposers see the Fed being compensated for their role in the FPN on a go-forward basis.

All users must enroll into the Directory. Not ideal for consumers. Should provide ease are auto enroll for consumers through financial institution.

While the proposal may appear efficient on the surface, so many of its assumptions are unlikely to meet either market or regulatory acceptance that it is impossible to determine the system's efficiency. For example, they posit the Fed as the issuer of the scheme’s "Fednotes" cash. If the Fed doesn't want to assume this role, which I would think is more than likely, the scheme has no stated alternative. Being unable to operate due to missing attributes seemingly necessary to stay in operation is certainly not efficient.

**Safety and Security**

Concern with dispute process in that all responsibility is placed on payer with no clear option for chargeback options particularly in the case of fraud/identity theft. How are situations handled if the payee is not willing to return the erroneous deposit? What is the recourse?

Due to its batch processes and returns processes, ACH inherently poses settlement risks to any financial institution in a faster payment environment—even if it is an ACH credit. As a funding mechanism in a real-time environment, the proposal should a) elaborate on how the FPN addresses and mitigates these risks associated with ACH delays and returns, and b) how the potential difference in settlement timeframes between the two proposed settlement mechanisms (ACH vs. API) impacts liquidity risks system-wide.

Use of contextual tokens likely provides a high level of data protection. The use of push payments and the fact that the payer only needs to know the payee's payment address should drastically reduce the use of sensitive credentials. FPN supports a variety of effective authentication methods, passwords, PIN, cryptographic keys, etc., biometrics.

Like the proposal to endure the FED to take an active role in the oversight of issuing and controlling the FED Notes Digital Money Supply within this proposal. Given the potential to create and issue billions of
web addresses—the FED Notes, would like to know more about how Wing Cash or its operating partner will secure and protect the ownership records.

Observation: this solution screams DDOS Attacks to potentially disrupt ongoing operation, customer trust/confidence, and ultimately adoption.

Not best solution for secure funds. Proposer holds funds. No answer for risk or protection of those funds for consumer or financial institution.

The idea of using unique URLs is very creative. Can these truly be secured for the purpose you propose?

S.4 Settlement –Concerned about reliance on Fed and viability of this solution if they don’t take on required role.

As with the other criteria, it is hard to gauge the proposal's safety and security because how the system would actually operate is described with so many likely to be unachievable assumptions and alternative ways of operating aren't provided, so there are no alternative safety and security factors if the parties on whom the scheme depends won't be offering them.

**Speed (Fast)**

This is a great strength of your solution. Nice work.

"Fast" is most certainly a relative term. Although the accumulated delays of a few seconds for each transaction is not so much an issue in the ATM channel, other aspects of speed are. One of the big advantages for the ATM channel that we see in this solution is its similarity to physical cash. Transactions are approved, cleared, and "settled" immediately and are irrevocable. These are important aspects of an ATM transaction.

Does the system provide any type of admin and service messages?

One would assume it would be instant, but like so much of the rest of the scheme this would depend almost entirely on the actions of other parties the scheme doesn't control.

**Legal**

Consumer protection is a concern for how the solution is basing all responsibility of the solution on the payer. This can have a large impact on FIs who will likely have to absorb these losses.

Reliance on revisions to the Federal Reserve Act in order for the solution to be compliant with regulations can impact the implementation of this solution. If the Act is not revised, what are other options in order for the solution to be viable?

Not an enriching comment, but thank you for addressing the legal framework.
The solution could be enhanced that details the consumer protection offered to consumers when utilizing the FPN network.

It was difficult to understand how the variations in the 3 organization structures (introduced on pages 136-137) would change any of the capabilities, benefits, or responsibilities previously mentioned in the paper (e.g., where the responsibility of CIP verification lies greatly affects the ease of use, cost, and social value derived by its participants). To avoid confusion, the paper should introduce the 3 legal structures earlier in the paper AND select only one to guide the reader through the proposal (i.e., “for the sake of the efficiency, this proposal assumes option X”).

How do digital notes relate to physical notes? Does Fed now have two independent monetary supplies to manage? This was asked in the live November session, but was not sufficiently answered and it will have a very large impact either way.

No discussion of BSA vetting by the Fed which would hold the accounts. Discusses minimal information from businesses to enroll so as to foster acceptance by 2020. Seems counter to new beneficial owner requirements for business accounts at banks. While a mitigating factor is a limit on transaction amounts, need to contemplate high volume, low dollar activity.

Fraud is said to be mitigated by strong authentication, but should consider a more layered approach.

What happens to the Fed notes a business or person is holding in the event of a business or personal bankruptcy or law suit?

Trying to issue a new form of specie in the U.S. might present legal challenges.

**Governance**

Not an enriching comment, but thank you for addressing the governance framework. I think the idea of the FPTF and SPTF serving as a possible governing organization is SPOT ON!!!

The solution appears to include an inclusive governance process, with a governing body composed of a diverse group of individuals that are representative of the diverse classes of participants using the platform. It also includes a public comment period, akin to the APA, which creates a heightened standard of transparency.

Like the proposal to ensure the FED to take an active role in the oversight of issuing and controlling the FED Notes Digital Money Supply within this proposal. The FED owning the Digital Ledger seems to fit their role with regards to this solution.

This proposal relies on the willingness on the part of the Federal Reserve Bank to be the operator of the system and the issuer of the Fednotes.
G.1 Effective governance & G.2 Inclusive governance, SOMEWHAT EFFECTIVE. They are proposing a membership Governing Organization (GO) to include FPN stakeholders “individually and collectively.” The proposer expects the Federal Reserve to be the rule making/governing body.

Other than positing the unlikely assumption that the Fed would run it, how the scheme would be governed is not clear.
WingCash response to Task Force Comments
Introduction
As we reviewed the comments from the task force, we found that the feedback fell into the following categories:

- Involvement by the Federal Reserve
- Financial Viability
- Business Model
- Governance
- Time Frame to Achieve Widespread Adoption
- Fraud Mitigation
- Disputed Payments

While many of the comments were written as statements, we rephrased comments as questions and then provided an answer for each question. For example, one commenter wrote, “It would appear that cash out would be another impediment,” and we turned this into the following question: “How does someone holding Fed notes on the FPN cash out?” We combined comments and questions that dealt with the same issue into a single question.

Involvement by the Federal Reserve

Does the Fed have authority to issue digital bills and coins?

Digital banknotes should be treated as authorized by the Federal Reserve Act to the same extent as physical banknotes.\(^1\) Section 16(1) of the Federal Reserve Act is silent as to the medium in which Federal Reserve notes are to be issued. Accordingly, it may be argued that digital banknotes are encompassed within the general authority of Paragraph 1.\(^2\) Digital Fed notes would not replace physical bills and coins but would be an additional service offered by the Fed.

Do the people want the Fed to play a role?

The people want a financial system that serves their purposes and protects their interests. If the FPN provides an additional option for payments that is easy to use, secure, cost-effective, and accepted by the establishments that consumers do business with, they are likely to accept it without a lot of consideration for the mechanics that make the system possible.

We are assured that not all consumers or businesses would like to have the Fed provide digital bills and coins for the FPN; however, consumers and businesses are best served

---

\(^1\) Faster Payments Network Solution Proposal, WingCash, LLC p.138  
\(^2\) Faster Payments Network Solution Proposal, WingCash, LLC p.139
by a safe, efficient, trusted payment ecosystem. The Fed’s role in the FPN would bring the highest levels of public confidence to the FPN.

**Will the Federal Reserve adopt the FPN?**

The Proposer cannot speak on behalf of the Federal Reserve; however, the Fed’s operation of the FPN would provide the highest level of credibility and trust in the FPN.

One of the strengths of the proposed FPN is its flexibility with respect to the role of depository financial institutions in the chain of distribution of digital banknotes. For example, the Fed could engage depository institutions to act as intermediaries with respect to the distribution of digital banknotes, similar to their role with respect to the distribution of paper Federal Reserve notes.

Administration of the Global Directory Service, the “back-office” machinery necessary for authentication and recording, and numerous other aspects of the Faster Payments Network, may be delegated to the Governing Organization or a service provider as the Fed sees fit. The proposer’s intent is not to dictate whether or how the Fed may exercise its discretion to delegate operation of the various components of the FPN; rather, where the FPN contemplates operative concepts from the point of view of Fed action, it should be understood to refer to action by the Fed or its designee, and not to derogate from the Fed’s flexibility to delegate or otherwise involve the Governing Organization, its members, or other third parties as necessary or appropriate to provide the FPN.

**If the Federal Reserve chooses not to adopt the solution, what are other options that could keep the solution viable?**

The multi-issuer design of the FPN makes it possible for a commercial bank to act as distributor of the Fed notes held against a balance in an omnibus account; however, our experience suggests that commercial banks resist this role and responsibility for many reasons. In the model with one or more commercial banks as providers of the notes, the Fed would not need to act as the issuer or redeemer.

**Financial Viability**

**How is the FPN paid for?**

The Federal Reserve can expect to receive full recovery of costs over the long run by directing savings from reduced printing, transportation and destructions costs of physical bank note issuance into the operation of the FPN. However, the implementation of the FPN would require an investment by the Federal Reserve.

**What revenue streams exist to pay for the operation of the FPN?**
The Federal Reserve will continue to recognize seigniorage for Fed notes issued to the FPN. We also propose other possible revenue streams associated with the FPN, although we do not prescribe who will record the revenue, as follows: distribution of brand cash, co-branding of Fed notes, deposit fees, education and training, membership, and more.

*Will the likely reduction of revenue in existing payment systems make the stakeholders of those systems resist or be slow to adopt the FPN?*

Yes, we expect stakeholders of other payment systems to be slow to or resist adoption of the FPN because of the potential loss of revenue as payments shift from existing payment systems to the FPN. However, financial institutions will be able to realize additional revenue by determining the fee charged to the customer for depositing Fed notes to an account. Depository institutions using the API with their own branded applications are able to offer the baseline services and value-added services for their customers. Value-added services may generate revenue for depository institutions.

*Will financial institutions have to absorb losses from the system?*

No, unlike payment card networks, the proposed design and rules of the FPN do not have financial institutions responsible for chargebacks. Financial institutions will benefit from reduced risk of payments that use the FPN because there is no inter-provider credit or liquidity risk when accepting Fed notes for deposit.

**Business Model**

*Are consumer or business accounts on the FPN the same as a checking or savings account at a depository institution?*

The FPN is designed as a bearer instrument payment network. The FPN is not a system of accounts that use double-entry accounting (e.g., debits and credits) to move value between accounts. Consequently, the FPN does not compete with depository financial institutions for deposit accounts of consumers or businesses.

*Can the FPN handle the billions of web pages needed and the transactions necessary at scale?*

The FPN will create and store data for each Fed note on the FPN. While this may seem like a lot of data, even with billions of Fed notes, it is rather small by comparison to some existing web sites. For example, YouTube reports that “every day people watch hundreds of millions of hours on YouTube and generate billions of views.” Serving hundreds of millions of hours of YouTube video places a high demand on computing resources (i.e., computer processing power, network bandwidth, and storage), whereas
the FPN’s serving static/dynamic web pages demands significantly less computing resources.

The FPN can scale quickly while maintaining service level agreements and providing the baseline core features because of an original design architecture that supports high scalability.

The proposers have tested the transaction throughput of the current open source version without much code optimization using Amazon EC2 Type C3 instances with 32 cores and 60 GB of memory. The current open source version was able to achieve projected annual transaction throughput rate in excess of 23 billion transfers per year (750 transactions per second, 64.8 million transactions per day). To put this in perspective, VocaLink, the operator of the UK’s Faster Payments system, indicates on their website that their data centers process just over 6 billion BACS transactions annually (16.44 million per day), with a peak reaching 100 million transactions per day (36.5 billion transactions annually). The proposers believe that, with both hardware and software optimizations, the transaction throughput of the FPN at implementation can be improved to reach or exceed 220+ billion transfers per year, or 602.7 million transfers per day. The FPN’s architecture is designed to accommodate growth with additional code optimization and through horizontal scale.

**Can the FPN be protected from DDoS attacks?**

The FPN includes the following measures to mitigate the impact of external network attacks:

- Because attackers often try to connect to database servers directly through network ports, the FPN employs external firewalls that reject all attempts to connect to non-public ports.
- The FPN mitigates denial of service (DoS) attacks by providing flexible server capacity and by adjusting firewall rules in real-time to temporarily block specific abusive IP addresses.
- The FPN serves static copies of web pages in the event of an extreme DoS attack. Because copies of static web pages require few server resources, it is more difficult for attackers to overwhelm servers that serve static copies of web pages.
- The proposers recommend the creation of a site reliability engineering (SRE) team to monitor the network and build automated detection and response systems.

**Does the FPN operate differently within government agencies, or are they treated like other businesses?**
The FPN operates the same for government agencies as with public/private businesses; however, the API allows a degree of freedom to a business or government agency to customize the features or experience of the FPN. Government and charitable organizations that distribute humanitarian aid would have the option to distribute a closed-loop payment instrument (Brand Cash) redeemable only at certain locations to provide better control of where humanitarian aid is redeemed and for what products and services.

**How does the FPN enable providers of core banking systems to enable domain aliasing capability?**

The FPN's domain aliasing capability allows FPN features to be aliased to the web domain of a financial institution. For example, a financial institution with a domain of www.firstfinancialinstitution.com could be set up to provide its customers customized, branded access and user experience to the FPN at fnp.firstfinancialinstitution.com.

**Can the FPN be modified to allow consumers to auto-enroll through their financial institutions?**

While it would be convenient, it is not to the consumers’ benefit to be auto-enrolled in the FPN through their financial institutions. The FPN enrollment process enables participants in the system to specify their credentials and keep them private. Enrollment that is not linked to a financial institution also expands access to the solution to unbanked individuals. For convenience, the FPN allows those who have accounts with depository financial institutions to link their payment addresses to their accounts.

**Does the FPN have settlement risks related to batch processes?**

Transactions within the FPN are immediate and are performed with good funds (i.e. central bank money) that are currently held by the payer’s primary payment address. The purpose of the FPN is to execute transfers in real-time, all day, every day without human intervention and provide confirmation of the completed transfer to both the payer and the payee.

**How does someone holding Fed notes on the FPN cash out?**

A user on the FPN can link an account at a financial institution to her primary payment address and submit a payment order to transfer Fed notes to that account. Users can purchase goods and services with funds held by their primary payment address. Fed notes on the FPN are also fungible with physical bills and coins.

**Does the FPN provide messages to inform users of transfer options and details?**
The FPN displays contextual data to inform users. The FPN records, retains, protects, discloses, and makes available to the payer, payee, and issuer appropriate contextual data as permitted by the rules. Contextual data may include but is not limited to the following:

- Transfer identification (each transfer is assigned a system-wide, unique ID)
- Transfer type (transfer types as defined by the system)
- Date and time the transfer was started
- Date and time the transfer was completed or ended
- Status of the transfer
- Amount of the transfer
- Visibility of the transfer (i.e., public or private)
- Appropriate details about each participant or stakeholder involved in the transfer
- Fed notes involved in the transfer by unique identifier
- Closed-loop notes involved in the transfer, including the type of the note (e.g., gift, loyalty, rewards, promotional), the name the notes Issuer, the denomination, and the date of issuance

The FPN may also capture and record contextual data that include channel- and device-specific information. For example, data may include device operating system, device hardware identifiers, device application identifiers, or device location information.

Contextual information associated with a transfer can be viewed by a stakeholder of the transfer to perform all types of responsibilities including updating double-entry accounting systems, preparing reports, preparing tax statements, auditing, and investigating errors.

The FPN enables flexibility in contextual data and integration of data and messaging with external systems.

What happens to the Fed notes a person or business holds in the event of a bankruptcy or lawsuit?

The Fed notes held by a person or business would be subject to all laws, regulations, and court orders, just as any other financial asset in the case of a personal or personal bankruptcy.

Governance

Who would have rule- or regulation-making responsibility for the FPN?

The same organizations that write regulations and laws for payment systems that exist today would have the ability to impact the FPN’s rules. These organizations include the
Furthermore, the solution proposes an inclusive Governing Organization with broad participation from all stakeholders on the FPN to also have rule-making influence.

Who has responsibility for compliance with BSA/AML/OFAC/KYC requirements?

The Fed would bear the responsibility for compliance with regulations in the ongoing operation of the FPN with established users. As the owner and operator of the FPN, the Fed could designate certain responsibilities to be performed by the Governing Organization. Compliance with BSA/AML/KYC may be delegated by the Fed to the Governing Organization.

Financial institutions that are issued digital Fed notes from the Federal Reserve would be authorized to redistribute the digital banknotes to customers who have satisfied anti-money laundering (AML) and Office of Foreign Assets Control (OFAC) screens. Moreover, the recipients of those digital banknotes would be able to transfer them only to persons (individuals and entities) whose identity had been validated in accordance with applicable AML and OFAC standards by banks authorized by the Fed for that purpose.

With strong front-end identity verification requirements, the FPN would enable AML-related controls far exceeding those currently in place for cash transactions. In addition, the FPN architecture supports a multi-tiered approach to the user base, with holders who have not undergone bank identity verification subject to hard-wired transactional limits (e.g., based on the number or dollar value of transactions during a specified period), while holders who have undergone screening may be subject to less stringent limits, or, if the digital banknotes held by such users are linked to an account, no limits other than restrictions applicable to those of any other holder of a bank account (e.g., standard OFAC blocks and suspicious activity reporting). Such a multi-tiered approach would both preserve widespread access to digital banknotes, and allow financial institutions to maintain their gatekeeper role for transactions at levels designated by the Fed.

Time Frame to Achieve Widespread Adoption

How long would it take to implement the FPN?

Although there is a open-source version of the FPN operating in the market, if adopted by the Federal Reserve, the proposer recommends replacing open-source applications with commercial applications. The proposer estimates that the process of replacing open source applications with commercial applications and preparing the FPN to operate at scale may take between 9 to 18 months. This period of technical preparation will allow time for the Governing Organization to ratify the rules for the FPN, and large merchants
will have the necessary lead time to prepare their systems for acceptance of FPN payments and distribution of Brand Cash.

**Is the timeline to achieve widespread adoption, as outlined in the proposal, reasonable?**

The solution proposal includes a timeline to achieve widespread adoption that is based on the work streams of the Task Force, which have undergone some modifications during the solution proposal process. It is a high-level timeline. Upon adoption of the solution, a detailed timeline would be developed with input from stakeholders. The detailed timeline would include milestones for governance, legal and regulatory requirements, design, implementation, and adoption by governmental and private key players, including the Fed’s issuing of digital Fed notes, merchants’ implementing the solution, and consumers’ being able to use it for payments.

**What proof-of-concept testing has been already done?**

The technology to support the FPN has been in development since January of 2009 and operating in local markets since 2011. The current open source version is interoperable with existing payment systems, including the ACH network, the payment card networks, the bill pay networks, and other payment networks.

The following features have already been implemented in the open-source version of the payment platform:

- Enrollment for persons in the U.S. and other countries as permitted by the rules
- Enrollment for businesses in the U.S. including federal, state and local governments, retailers, etc., and for businesses in other countries as permitted by the rules
- Enrollment for depository institutions in the U.S. and in other countries as permitted by the rules
- Enrollment and support for national currency issuance by central banks in other countries as permitted by the rules
- ACH network integration and support for transfer of funds to accounts held at depository institutions
- Support for businesses and governments to issue closed-loop value (e.g., gift, loyalty, rewards, promotional, humanitarian, and welfare programs) with offers and campaign tracking (Businesses administer their own closed-loop networks with appropriate distribution and redemption agreements for network participants.)
- Support for sharing data using open data sharing formats, including a live web page (e.g., HTML5), Atom, JSON, and streaming
- Open API using OAuth2 for integrators
• Features to support customized branding by depository institutions and regulated non-bank providers using domain name aliasing and themes
• Reports, including transfer history, page groups, provider liabilities, distribution and redemption, received, and receivable
• Support for businesses to have payment addresses with public information published in the Global Directory Service
• Automatic sweep to deposit account with a fixed fee per sweep
• Administrative features include:
  ○ Payment address management
  ○ Enrollment management
  ○ Transfer analysis

In addition to the above features’ already have been tested in an open-source implementation of the platform, the FPN’s design would maintain the business relationships that exist between stakeholders. For example, depository institutions are members of the Federal Reserve System and order Federal bank notes from the Federal Reserve; with the introduction of the FPN, depository institutions will be transferred digital Fed notes electronically rather than receiving printed notes by armored car services. Depository institutions also maintain the relationships they have with their customers (e.g., provide customers with Fed notes when requested and accept Fed notes for deposit). Regulated non-bank providers maintain the relationships they have with their customers (e.g., cash advances, loans, check cashing). Businesses also maintain the relationships they have with their depository institutions and their customers. The FPN is a platform to enable transfers between all parties enrolled without requiring modification of existing relationships between participants.

Fraud Mitigation

How are the records of ownership protected?

The records of ownership of Fed notes can be protected by using a distributed ledger to record a hash of details for a transfer at each step in the work flow and a hash of the completed work flow and final transfer. While the hashed information can be written to a public distributed ledger without disclosing private details about the transfer, permissioned parties are able to store an independent copy of the hashed information and verify it against the transfer details to protect and verify the integrity of the FPN.

What protections does the FPN offer consumers?

The solution protects the personal information for end users, the Fed notes they hold, and transaction details by encrypting data in transit and at rest.

The FPN encrypts data in transit as follows:
- Data in transit between servers and clients is encrypted using Secure Hypertext Transport Protocol (HTTPS) using Transport Layer Security (TLS) consistent with the guidelines published by NIST.
- Data in transit between servers is encrypted using TLS encryption.
- The FPN uses a Virtual Private Network (VPN) to secure the communications for some administrative processes and services.

The FPN encrypts data at rest as follows:

- Certain records at rest in the database are hashed (e.g., passwords) using secure hashing algorithms consistent with guidelines published by NIST.
- All data at rest on hard drives are encrypted using algorithms based on Advanced Encryption Standard (AES), a NIST-adopted standard.

The solution’s risk management framework also protects consumers from fraud in the following ways:

- The FPN uses push payments exclusively instead of allowing the payee to pull from the payer’s payment address.
- The FPN does not share sensitive information (e.g., account numbers, card numbers, personal information, etc.) with the payee.
- In contrast to checks or payment cards, only known individuals with valid payer credentials are authorized to access the payer’s payment address and to sign payment orders.
- The FPN offers the Federal Reserve and the Governing Organization ability to regulate and oversee the function and operation of the system including the ability to analyze the source, destination and amount for all transfers in lieu of identity verification for every individual.
- The FPN supports optional two-factor authentication that when activated assures that the individual authenticating is also in current possession of protected secret information (i.e., token generated from biometric information).
- The FPN’s payment order dialog supports reverifying the presence and possession of the secret information (i.e., token generated from biometric information) before the payer’s signature will be applied to the payment order.

*Why does the FPN allow single-factor authentication?*

The FPN also employs a username and password or passphrase pair as a method to verify an end user’s identity to satisfy end user expectations. End users can establish multi-factor authentication for enhanced security. Additional means of authentication can include one-time passwords using a secondary communication channel (e.g., sms/text message), one-time passwords using a separate application (e.g., VIP Access from
Symantec, Google Authenticator) or a device that displays the one-time password (e.g., Security token or card), hardware key using PKI (e.g., Yubikey) and biometrics using mobile devices. Additionally, the FPN may require an end user to activate multi-factor authentication as required by some business processes and security features (e.g., a business may require all managers to use multi-factor authentication to sign a payment order).

Who has the liability for funds held by consumers or businesses on the FPN?

The United States would have liability for Fed notes held by users of the FPN.

How does the FPN incorporate a layered approach to fraud mitigation?

The FPN is designed with robust measures to prevent fraud. In addition to incorporating mechanisms to prevent fraud before it occurs, the FPN includes backend, real-time monitoring to spot exceptions that may indicate fraudulent transactions. The GO and those responsible for managing the FPN’s operations will analyze the exceptions data, then determine, develop and implement the correct response for handling exceptions that have been identified. For example, the fraud detection group may discover a common pattern of individuals transferring small amounts among many payment addresses to hide the possession history, then aggregating the value into a single payment address to be spent or deposited into an account at a depository institution. In response to detecting this sort of pattern, the fraud detection group could write and implement processes and procedures to suspend payment addresses that are participating in the detected pattern. Suspended payment addresses could then be evaluated and investigated.

Disputed Payments

Who is liable for erroneous payments?

As with physical cash payments, payers who use the FPN are liable for erroneous payments. The proposer believes that, while there is some risk to consumers within such a system, the benefits of the FPN (speed and reduced transaction costs) outweigh those risks. A payer must authorize a payment order before Fed notes are transferred to the payee. The FPN requires the payer to present credentials on the system before submitting payment orders, and it clearly communicates that the payment will be immediate and irreversible. A payer is responsible to protect his credentials as carefully as he would protect his wallet if he were using physical cash.

The FPN should be seen as an option for payers to supplement the payment options currently available. The FPN is an appealing alternative for transactions, such as purchasing fuel at a pump, where the payer has no need of additional consumer
protections, has no misgivings about making an irreversible payment, and may reap benefits of reduced costs. A payer who has misgivings about irreversible payments may choose other, existing payment systems that have costs associated with these protections built in.

*What is the recourse for a payer if goods or services provided are not satisfactory?*

Payers who use the FPN have the same modes of recourse as payers who use physical cash payments. They can work with the payee to arrange a refund. Payees are motivated to maintain their customers' good will, so it is reasonable to assume that this mechanism for resolving disputes will be satisfactory most of time. Then if the payee is fraudulent or not cooperative, the payer can work through existing systems, such as the court system, to recover losses. While these mechanisms are more onerous than calling a financial institution and demanding a refund of disputed payments, the payer who uses the FPN does not bear the burden of the hidden costs associated with existing systems that shift financial liability for such transactions to financial institutions, which must then recover their costs by charging higher fees to customers.

**Conclusion**

The proposer believes that the Faster Payments Network is a viable solution for faster payments with the benefits and features sought by the Task Force. The proposer understands that adopting a new payment system is a significant undertaking and has sought to address the questions and concerns raised by the Task Force, beginning with the reasons why it would be beneficial for the Federal Reserve to adopt the FPN and including details about the financial viability of the solution, the business model, governance, time frame for adoption, fraud mitigation, and disputed payments.

The proposer believes that by issuing digital currency and supporting the FPN, the Federal Reserve will be providing a service that the Fed is uniquely positioned to enable—one that will facilitate clear public benefits through broad-based, non-discriminatory access to an efficient and effective means of electronic commerce and that will enable the Federal Reserve to continue to perform its core responsibilities in managing the money supply. The FPN is competitively neutral and cost-effective and will enable the Federal Reserve to continue to ensure the integrity of the payment system with modest changes to existing law. The proposer respectfully submits that the Faster Payments Task Force and the Federal Reserve should adopt the FPN as its primary initiative for payment system improvement.
Faster Payments QIAT

FINAL ASSESSMENT

Proposer: WingCash

Summary Description of Solution:
The WingCash solution, known as the Faster Payments Network (FPN), is a software platform that, as proposed, would be owned and operated by the Federal Reserve Bank and “the Governing Organization” (GO). The proposer recommends that the GO comprise members of the Faster Payments and Secure Payments Task Forces.

The FPN uses a digital currency for payment. This currency, called “digital Fed notes,” would be issued by the Federal Reserve and is tied to the Federal Reserve Bank’s Internet domain (Fednotes.com). The Federal Reserve would control the digital Fed notes, but authenticated individuals and businesses would be able to hold, transfer possession of, and deposit these notes.

The solution’s end-to-end payment process begins with a person or business enrolling in the FPN, then continues through the iterative steps of authentication, payment order, receipt, and optional reconciliation upon conversion or redemption of Fed notes in U.S. dollars or other currency. Changes in possession of the FPN occur directly between payer and payee without transfer fees.

Each digital Fed note is a unique webpage with an unchangeable URL (e.g., fednotes.com/usd/ml14060622c) with a single, permanent monetary value. In addition to the URL, each Fed note is assigned a single, permanent, monetary unit of value (e.g., $0.01 to $100). Because these notes are similar to cash, they could be used as cyber-currency or stored in digital wallets. Fednotes.com would publish the digital Fed notes, each of which would include the issuer’s URL and the current holder’s URL, which would point to the holder’s profile unless masked for privacy reasons.

The FPN is thus a system of payment addresses (URLs), not accounts. Payments would be transacted by changing the possession of each Fed note—i.e., changing the owner of the URL. The URLs, which are mapped to a payment address or payment address alias, such as an account at a depository institution, would be stored in a “Global Directory Service” (GDS).

The technical design of the FPN allows businesses to issue closed-loop value in standard denominations. The proposal refers to this as “brand cash.” Brand cash is restricted as determined by the issuer and FPN rules, and the digital note includes the issuer (e.g., the business name), the redemption locations, the holder, and other information.

EXECUTIVE SUMMARY OF THE PROPOSAL

- Major strengths
  - This digital currency solution increases accessibility by enabling all end-users (individuals acting on their own behalf or on behalf of a business) to enroll directly through the FPN enrollment
page (e.g., fednotes.net/signup), essentially creating user payment addresses in a ledger directly with the Federal Reserve.

- Features such as brand cash for closed-loop currency; enablement of the payee to require the payer to present a unique payment code before a transfer can be completed; and the ability to customize an individual payment address and share it publicly on social media can all increase adoption and allow the solution to be used across a range of use cases, including POS (point of sale).

- Based on the videos of end-user experience shared in the proposal, the solution is highly usable and predictable.

- The solution provides real-time funds availability and enables immediate settlement through digital notes, thereby minimizing credit and liquidity risk. It is designed and engineered to prevent fraud and minimize user errors. No personally identifiable information (PII) is handled or exchanged during transactions, further mitigating risk.

**Areas for improvement and enhancement**

- The solution hinges on the willingness of the Federal Reserve to own and operate the FPN (and create new monetary policy). Unless Fed notes become legal tender, adoption rates may lag, since depository institutions would give up revenue associated with current payment systems, and new security and technical infrastructure would need to be built.

- The proposal described several models for Fed notes distribution, some of which have weaknesses. In the first, a “bank-centric” model, the Fed issues digital notes to banks, which then redistribute digital notes to individuals. The identity verification needed to assign payment addresses would be the responsibility of the GO rather than the bank. In the solution’s “bank-light” model, the Fed is responsible for validating the identity of payers and payees. The solution’s hybrid model envisions multiple tiers of transaction authorization based on the level of identity validation. The proposal notes that the Federal Reserve is more likely to select the bank-centric model since it is more consistent with the current mode of operation, takes advantage of bank relationships with customers where identity has already been validated, and avoids the Federal Reserve having to undertake customer identification programs.

  In the bank-centric model, providers need sufficient motivation or incentive to adopt the solution and make it available to end-users. Moreover, making the GO responsible for identity verification of all users poses a significant build-and-execution challenge.

  - The solution requires the capacity to issue and hold billions of web addresses, creating a security and scalability challenge for the Federal Reserve and GO to jointly manage.

**Use cases addressed**

- FPN addresses all domestic and cross-border use cases, including B2B (business to business), B2P (business to person), P2B (person to business), and P2P (person to person). It also covers closed-loop notes.

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

- The solution has already been deployed on a smaller scale and has a proven track record. The proposal provides videos that demonstrate the user experience. However, the solution depends on Central Bank adoption to issue digital fiat currency and to act as the operator, as well as on regulatory changes.
## 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 Fast Payment Network (FPN) is easily accessible to all U.S. consumers and businesses (U.1.1). It does not require a bank account (U.1.4); users directly enroll and need only to provide basic personal information (e.g., name and address) and to choose their authentication approach—such as a password, a hardware key, or a biometric token. Anyone can establish a unique identity and token. In addition, any recipient can receive a payment (U.1.2); if a recipient is not enrolled in the solution, he/she receives an invitation with instructions to enroll before receiving the payment. Users can also transfer or deposit their Fed notes to checking or savings accounts at depository financial institutions. The FPN supports multi-currency by having other central banks or financial institutions issue national currencies to the GDS (U.1.3).

The solution’s plan for achieving widespread adoption relies on the Fed to operate and issue Fed notes as legal tender, to gain the trust of individuals and entities using the FPN, and to assure overall public confidence. The implementation plan includes obtaining commitments from top retailers (who can issue closed-loop value and utilize branding opportunities in FPN) and depository institutions (which will be motivated by branding opportunities, reduction in costs, and a potential fee for distribution or deposit of Fed notes) (U.1.5).

While end-users often use physical cash for its anonymity, anonymous transfers are not possible in the FPN, which could create adoption challenges. The FPN does, however, enable privacy for transfers; for example, each Fed note, under the rules, may not be required to publicly show the end-user’s identity. The solution plans to drive end-user adoption of digital currency through a value proposition based on accessibility and ease-of-use, free transfers, ability to hold and redeem closed-loop value, the solution’s personalization and social media aspects (the ability to share payment addresses), and the public’s trust in the Federal Reserve.

### 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 demonstrates a straightforward, simple end-user experience (U.2.4) that is available 24x7x365 through email, phone, a social media address, or the payee’s primary payment address in the directory—as long as the user has a device and an Internet connection (U.2.1, U.2.3). To enroll, users need only to provide basic personal information (e.g., name and address); they are then assigned a unique identity and token with which to make payments (U.2.2). The FPN’s technical design enables initiation of payments through email, phone number, social media address, a payee’s primary payment address, a payee’s custom payment address in the GDS, a widget on a website, or a published application. The solution’s design accommodates varying levels of technological proficiency and addresses the needs of individuals with disabilities, the elderly, and those with limited English proficiency (U.2.4). In addition, payment status is transparent to users at every step of the transaction (U.2.3).
### 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 FPN clearly defines its baseline features, which are delivered consistently and centrally by the Federal Reserve and the FPN’s Governing Organization (GO) (U.3.1, U.3.4) and comply with the relevant laws (U.3.2). The solution communicates transactions’ costs and implications to end-users before the transactions occur (U.3.2), as demonstrated by the proposal’s visuals. The solution employs Internet-standard communication and messaging protocols (U.3.3) but allows providers to customize their user interfaces.

The solution clearly defines error resolution protections, rights, and liabilities and makes those easy for payees to understand (U.3.5). It also defines mechanisms to reduce the incidence of unintended payments (e.g., message prompts to the payer to confirm payment to a new recipient). Several generic terms are provided to distinguish the solution from other payment methods such as digital banknotes and Fed notes (U.3.6).

### 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 FPN supports contextual data, including the data fields identified on page 79 of the proposal (U.4.1). The proposal indicates that the Fed and Governing Organization will determine the actual message formats and data dictionaries to be supported at implementation. While the default message format of the FPN is JSON (Javascript Object Notation), the technical design translates data to other standard message formats, including ISO 20022.

The FPN facilitates easy integration with business and personal finance systems by enabling end-users to apply tags to transfers and to define data dictionaries for automated use with external systems (U.4.2). The solution balances the need for flexibility with the need for standards by allowing both unstructured and structured formats and by supporting data fields in a custom-defined data dictionary as well as the ISO 20022 standard (U.4.3).

More detail would be helpful on the ability of JSON to support the contextual data requirements of corporate (B2B) payments. Given the solution’s dependence on translation, the proposal needs to ensure that the translation engine is 100% effective and doesn't lead to errors or omissions.

### 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 FPN enables cross-border payments through its technical design, which allows rules, regulations and laws to be incorporated into the network logic (U.5.1). Interoperability with other
payment systems can only be achieved if those systems adopt the FPN and implement the necessary code changes to support their network’s rules and regulations (U.5.2). The FPN ensures that providers disclose exchange rates and fees to the payer (U.5.3) and enables conversion from one currency to another by allowing the payer to determine the currency to transfer and allowing the payee to convert the currency as desired through conversion exchange providers (U.5.4).

More detail would be helpful on how the FPN is compatible with other networks (such as ACH, the card networks, Dwolla, and Ripple) as noted on page 81 (U.5.2). The implementation plan for cross-border capability is rooted in confidence that, if the U.S. adopts digital currency, other countries will follow, but further detail would be helpful on any go-to-market plan for other countries’ issuing national currency as part of the GDS (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 FPN covers all use cases for both domestic and cross-border payments. Its target use case centers on P2P payments; many of the concepts and details of this use case can be extended to other cases as well. The solution would be enhanced by providing more detail on its applicability to corporate (B2B) 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:**
Because FPN transfers are free, competition among providers will be based on offering superior user experiences and value-added services that use the GDS and the FPN’s API (application programming interface) to extend the solution’s baseline features (E.1.1). End-users can choose the provider they prefer and use multiple integrator applications at the same time, but they can spend Fed notes only once. Switching integrators just requires opening another application, since the value of Fed notes displayed in the end-user’s mobile application is updated in real time to reflect the end-user’s transfer activity (E.1.2). Any provider with a feasible application that can integrate through the FPN’s API can participate (E.1.4) in the solution. The solution requires providers to disclose total costs to end-users in advance and provides strong examples of this capability (pp. 85-86) (E.1.3).
E.2 Capability to enable value-added services

Very Effective             Effective  Somewhat Effective       Not Effective

Rationale:
The solution allows any provider or “integrator” to provide value-added services through the use of an open API (E.2.1). Potential value-added services might include products such as “branded cash” (e.g., bank-branded frequent flyer miles). All providers that meet the participation requirements can be integrators and develop customer interfaces, software applications, mobile applications, and services (E.2.2). The FPN requires providers to clearly disclose to customers that the value-added services are optional (E.2.3).

E.3 Implementation timeline

Very Effective             Effective  Somewhat Effective       Not Effective

Rationale:
The solution has a track record, having operated with fully developed and market-tested features in other markets since 2011. The FPN’s implementation plan includes a plan for funding (describing both the funding required by the Federal Reserve and Governing Organization and how to recoup it through cost reductions associated with physical cash), implementation, and overcoming ubiquity hurdles. The plan delineates the entities targeted for first adoption of the solution (top retailers, providers), market share and growth projections, and the projected timeline compared to historical examples (E.3.1). The solution acknowledges that achieving ubiquity for a payment service by 2020 is unparalleled in recent history. The implementation plan depends heavily on three things: 1) the Federal Reserve’s commitment to owning and operating the FPN, as well as a Governing Organization that is capable of securely validating all users of the FPN; 2) robust adoption by businesses, billers, merchants that enroll in FPN, integrate at the POS, and issue closed-loop currency as an incentive for customers to pay with the FPN; and 3) the participation of providers as a distribution mechanism to customers who have a payment address linked to their account with the depository institution. In terms of incentives, the proposal mentions that banks can charge end-users a fee for distributing or transferring the FPN to their deposit/credit card accounts, but this incentive will likely be weighed against current revenue streams from the system.

E.4 Payment format standards

Very Effective             Effective  Somewhat Effective       Not Effective

Rationale:
The FPN’s standard message format, Javascript Object Notation (JSON), can interoperate with existing payment format standards through data translation (E.4.1). Given the dependence on translation, the solution needs to ensure that the translation engine is 100% effective and does not cause errors or omissions. The solution addresses the cost-effectiveness of the message format by
allowing integrators to choose their message format (E.4.3) and provides a mechanism for updates
by enabling data translations of various standard message formats to/from JSON (E.4.4). The
solution uses message formats published by recognized standards development organizations
(E.4.5).

E.5 Comprehensiveness

**Very Effective**

Effective Somewhat Effective Not Effective

**Rationale:**
The FPN’s solution is comprehensive, with simplifying approaches to traditionally cumbersome
stages. It enables all aspects of the end-to-end payment process, performing receipt, clearing, and
settlement simultaneously (E.5.1). Its technical design supports all of its features, including its
usability, reliability, performance, information security protocols, operations, compliance controls,
and risk controls (E.5.2).

E.6 Scalability and adaptability

**Very Effective**

Effective Somewhat Effective Not Effective

**Rationale:**
The FPN’s technical design supports projected use cases (E.6.1) and is based on web-based, open
standards. The technical design is adaptable, since it is based on Internet and open standards and
provides an API that integrators can use to address changing technology and customer-driven
demands. In addition, the Federal Reserve controls the solution through a single, universally trusted
and authoritative Internet domain and can drive the response to economic and regulatory
developments (E.6.3).

The solution today can reach a capacity of 23 billion transfers per year, but the proposers believe
that, with hardware and software optimizations, the FPN can handle 220+ billion transfers per year
(E.6.2). The solution uses distributed architecture that spreads the storage and query load among
many databases; however, the scalability required for implementation is unprecedented.

E.7 Exceptions and investigations process

**Very Effective**

Effective Somewhat Effective Not Effective

**Rationale:**
The solution provides an application layer protocol that allows changes in status of all network
applications to be monitored in real-time. In addition, an administrative tool can be used to identify
and resolve transfer errors, failed signup attempts, cancelled payment addresses, and other
exceptions (E.7.1). The solution ensures that information is created, recorded, and retained for a
period of time specified by the operating rules; information relevant to every transfer is captured
and stored (E.7.2). Exceptions data and transfer errors are captured in a centralized logging
repository. The FPN will use these logs to spot exceptions not visible to the individual participant.
The fraud protection group within the FPN will analyze exceptions and then determine the right response for handling.

More clarity on the protocols for addressing exceptions in a reasonable timeframe would be helpful.

Safety and Security

S.1 Risk management

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

**Rationale:**

The FPN’s risk management framework outlines the Federal Reserve’s roles and responsibilities and notes that the FPN’s architectural design is adaptable to law or regulation (S.1.1). The solution’s settlement approach mitigates risk because Fed notes act like cash, and no intermediary FIs need to transfer the money (S.1.2). The solution addresses measures to prevent and reduce the risk of unauthorized, fraudulent, and erroneous payments (S.1.4). For instance, payers must sign and reconfirm push payments at the time of payment, because the payment is irrevocable once it is executed. Since payments occur directly between payers and payees through the FPN, special incentives are not needed for providers to contain the risks they pose to other participants (S.1.5). The Governing Organization will ensure that the FPN’s risk management framework is subject to periodic review (S.1.6).

Several of the proposal’s descriptions of the risk management framework are rather general; in particular, more details are needed on how the FPN addresses operational risks (S.1.3).

S.2 Payer authorization

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

**Rationale:**

Because the FPN uses Fed notes, payers do not need to obtain authorization from their depository institution whenever they initiate a payment; instead, payers can directly pay payees without their depository institution’s acting as an intermediary (S.2.1). The solution allows payers to pre-authorize payments using payment codes, but this “pre-authorization” function does not include pre-authorization of payment on a future date, as that capability is not currently available (S.2.2-3).

S.3 Payment finality

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

**Rationale:**

Because users pay with digital Fed notes, which guarantee good funds, no depository institution needs to approve their payments (S.3.1). The transfer becomes irrevocable when the FPN displays a
confirmation page after the payment order has been executed (S.3.2). The FPN transfers the value before notifying the payer and payee.

The design principles of the FPN are intended to mitigate the need for an intermediary to resolve disputed payments. The proposal indicates that the FPN will have rules and regulations to protect payers and resolve disputes, but more detail is needed on the mechanisms and processes to protect or compensate the payer in cases of disputes (S.3.3).

S.4 Settlement approach

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

**Rationale:**

The solution settles payments in central bank money (i.e., digital Fed notes) (S.4.3). FPN’s transfers of the Fed notes do not incur settlement obligations between a depository institution and/or a Regulated Non-Bank Account Provider because the payments are sent directly from payer to payee (S.4.1). As a result, there is no inter-provider liquidity risk (S.4.2).

S.5 Handling disputed payments

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

**Rationale:**

The FPN’s approach to handling disputed payments focuses on best-practice processes and procedures to reduce errors and prevent fraud. The solution’s rules clearly state that the payer is accountable and financially responsible for all incorrect or erroneous payments (S.5.1). The solution does not include a consumer payer’s provider in the transfer of Fed notes (S.5.2). The payer and the payee can request a return of the funds, but the outcome depends entirely on the payee’s consent (S.5.3). The FPN’s approach to protecting business, government, and consumer payers from losses related to fraud or errors is to implement processes that reduce the chance of errors and fraud. Liability allocation when fraud or error does occur, however, is on the payer (S.5.5).

The design principles of the FPN are intended to mitigate the need for an intermediary to resolve disputed payments. The proposal indicates that the FPN will have rules and regulations to protect payers and resolve disputes, but more detail is needed on the mechanisms and processes for dispute resolution within the FPN (S.5.1).

S.6 Fraud information-sharing

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

**Rationale:**

The FPN streamlines the process of information-sharing by centrally collecting and aggregating information for all transfers under the Internet domain where the Fed notes are issued (S.6.1, S.6.6). The sharing mechanisms are based on standard data interchange formats and protocols and include
activity feeds available to participants and integrators (S.6.4). These sharing mechanisms enable real-time updates and alerts to participants (S.6.3). The FPN continuously logs, reviews, and monitors data about participants (individuals, businesses, and financial institutions), which enables the FPN to identify and evaluate potential risk patterns in real time system-wide (S.6.7). The solution then uses data analyses to determine and act on mitigating strategies. It employs a role-based permission system to control data-sharing (S.6.5).

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 FPN has layered, robust technical, access, operational, procedural, and managerial controls that address and foster security (S.7.1-3). These controls help protect and maintain the integrity of confidential, private, and sensitive data (S.7.1). Security controls are especially strong where the Federal Reserve and Governing Organization are responsible for policies, controls, and oversight. These strengths are particularly important for protecting the application layer, which will face continuing and intensifying security threats.

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 solution defines its target metrics and approach to resiliency, referring to the FPN’s availability as “five nines”—i.e., 99.999% (S.8.1). The solution ensures that those target availability metrics can be achieved through excess capacity, mechanisms, and technology to deal with DDoS attacks and other types of cyber-attacks. The implementation team will also develop and implement comprehensive business continuity and disaster recovery policies (S.8.2). The Governing Organization will ensure that sufficient resources are devoted to business continuity and resiliency and will also oversee the contingency planning process (S.8.5). To minimize the chance that adverse FPN-related events could cause other market participants to fail to meet their obligations, the solution has the Federal Reserve acting as the redeemer of last resort (S.8.3).

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 solution’s Global Directory Service (GDS) protects sensitive information and eliminates the need for payers and payees to exchange depository account information (S.9.1-3). The GDS stores all personally identifiable information (PII), which is then replaced by URLs—electronic addresses that link to payment card and account information but do not store it. These URLs are exchanged in the messages and used to process payments. All URLs are tied to the Federal Reserve’s web domain and become invalid if someone tries to use them outside this domain.
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 FPN requires robust identification and verification when enrolling and interacting with end-users and providers. It supports authentication methods that include identity-service providers, passwords set by end-users, PINs, and devices with cryptographic keys and biometrics identification (S.10.1). In addition, the GDS, payment codes, and the ability to conduct test transfers ensure that a payment reaches its intended payee (S.10.2). FPN aligns with regulatory guidance and industry standards for authentication (p. 128) (S.10.3).

The FPN also applies strong end-user authentication controls across all delivery channels and can vary the authentication procedure based on the risk-weighting of a given transaction (S.10.4-5). The API adheres to OAuth2. End-user authentication requirements can be based on an individual’s permissions in the FPN. The Governing Organization is responsible for ensuring that the FPN adopts new and decommissions old authentication models based on the evolving threat landscape (S.10.6).

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 solution outlines the participation agreement for providers that choose to participate in the FPN, including requirements around deposits, information systems, and regulatory and legal requirements (S.11.1).

The FPN does not require special participant requirements for depository institutions but utilizes the existing regulatory regime. The responsibilities and requirements associated with distributing Fed notes represent the only change needed for depository institutions (S.11.2).

The FPN Governing Organization will regularly monitor and ensure compliance with the participation requirements. In addition, the FPN will implement participation requirements in the software code as much as possible (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:**

Because payments are executed by transferring ownership of Fed Notes via their URL, they do not require the approval of the payer’s depository institution or regulated non-bank provider. This satisfies the Task Force’s “Very Effective” criterion of executing approval within two seconds.
Good funds are assured because Fed Notes are considered legal tender issued by the Federal Reserve.

F.2 Fast clearing

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

**Rationale:**
The FPN allows the payer and payee to exchange payment information in real time without requiring the depository institution or Regulated Non-bank Account Provider to exchange payment information. This satisfies the Task Force’s “Very Effective” criterion of clearing within two seconds.

F.3 Fast availability of good funds to payee

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

**Rationale:**
The FPN executes all submitted payment orders in real time and immediately displays a confirmation page to the payer indicating that the transfer is complete. The payee can withdraw or transfer these funds immediately. This satisfies the Task Force’s “Very Effective” criterion of making good funds available within one minute.

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

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

**Rationale:**
The solution satisfies the Task Force’s “Very Effective” criterion of settlement within 30 minutes because there is no lag in settlement with FPN transactions and thus no credit or liquidity risk for providers (F.4.1). Transactions are settled immediately upon payment confirmation (when possession of the digital Fed note is transferred from the payer to the payee), which can occur 24x7x365 (F.4.1). There is no lag when settling across different time zones (F.4.2). The FPN also allows payers to specify a later time for payment execution and will thus defer the payment, but the payment will still settle immediately at that later time (F.4.3).

F.5 Prompt visibility of payment status

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

**Rationale:**
The solution satisfies the Task Force’s “Very Effective” criterion of providing visibility into payment status within five seconds, as both the payee and the payer are notified immediately when
possession of the digital Fed notes changes (F.5.1-2). Once the FPN changes the possession of the Fed notes, it sends a confirmation of successful payment to the payer and the payee. The payee has good funds in digital Fed notes the moment those notes’ possession changes. If the FPN cannot change possession of the notes from the payer to the payee, it immediately sends an error message to the payer to notify them in real time that the transfer did not succeed.

Legal

L.1 Legal framework

**Very Effective**  Effective  Somewhat Effective  Not Effective

Rationale:
The proposal articulates a thorough legal framework for managing digital Fed notes and delineates the applicable laws and the changes that would be required (pp. 137-141) (L.1.1). The FPN has conducted several rigorous assessments of the framework and provides an extensive description of the legal sources, potential gaps in those sources, plans to close those gaps, and the means by which it will support compliance (pp. 146-151) (L.1.1-2, L.1.4). As part of this description, the proposal addresses potential revisions that might be necessary to the Federal Reserve Act and offers thoughts on those revisions (pp. 142-144). The proposal also explains how entities and payments through the payment system (from payer to payee) will be legally bound within the proposed legal framework for the solution (L.1.3).

L.2 Payment system rules

**Very Effective**  Effective  Somewhat Effective  Not Effective

Rationale:
The FPN has requirements, standards/protocols, and procedures that govern the rights and obligations of all end-users, providers, payers, and payees. The solution’s payment system rules cover all required features of L.2, including providing an error resolution process for end-users: payers are accountable and financially responsible for errors on signed and executed payment orders, while the Governing Organization has responsibility for resolving system errors (L.2.5). The process allocates to the appropriate entities the legal responsibility for obtaining valid authorization for payers, as the rules permit only the payer’s using valid credentials and acting on their own behalf to sign and submit an order to the payment system (L.2.4).
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 FPN has a legal framework and procedures that allocate legal and financial responsibility for losses in the event of a disputed consumer payment (L.3.1). It also provides options where it, end-users, and providers can establish additional consumer protections for payments (L.3.3).

The FPN is designed with strong protections to prevent fraud and errors. However, more clarity is needed on the support the solution provides for resolution of consumer claims arising from errors that do happen (L.3.2).

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 Governing Organization will establish and adhere to a privacy policy for the payment system. The policy will address when and how payment and related information can be collected and disclosed so that it is consistent with applicable policies, laws, and end-user preferences (L.4.1). The proposal describes the solution’s approach to ensuring the security of payment and related data—including legal requirements—and articulates various protections in place throughout the system (L.4.2). The nature and type of end-user data that may be required for security, legal compliance, and authentication purposes within the solution are described (L.4.3). End-users have visibility into the data collected on them and some control over the data being collected (L.4.4). The proposal is also clear about the responsibilities for data breaches at FPN, at the end-user, or at a provider (L.4.5). The Governing Organization is responsible for protecting against data breaches and threats. For instance, end-users are accountable and financially responsible for losses associated with the misuse or theft of their credentials.

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 offers an open-source version of the current embodiment of the FPN available at wingcash.org. On January 2011, the inventor conducted an international patent search for claims; the holder of the patents is willing to license or transfer the patent to the Federal Reserve or the Governing Organization under mutually acceptable terms. The FPN’s open-source application stack can be replaced with equivalent proprietary applications from other vendors to achieve the faster payment capabilities of the proposed solution.
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 proposal lays out governance arrangements that ensure efficient decision- and rule-making (G.1.1) and that provide a clear appeals process (G.1.3). These arrangements are publicly disclosed (G.1.2) and provide for independent validation of compliance with FPN’s rules, applicable laws, and achievement of relevant objectives (G.1.4).

G.2 Inclusive governance

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

**Rationale:**

The solution’s process for implementing new rules includes a commentary period from the public. In addition, the rule making committee must publicly describe how public comment was addressed in the rulemaking process (G.2.1). The FPN’s Governing Organization has a diverse composition, and the FPN provides all stakeholders with a chance for input and influence (G.2.2). The Governing Organization will create advisory bodies, including one for financial institutions, given their role as distributors of Fed notes (G.2.3). The FPN’s governance approach enables specific stakeholders or stakeholder groups to proportionately influence outcomes through representation within these governance and advisory groups (G.2.4). The solution addresses and manages actual, perceived, and potential conflicts of interest by establishing processes and methods to identify, disclose, and manage conflicts of interest; one of those mechanisms includes disqualifying members of the Board, executive team, or staff members from participation in official matters (G.2.5).