Faster Payments QIAT

Proposer: University Bank

February 21, 2017

TABLE OF CONTENTS

Original Proposal 2

Q&A Response 155

Draft QIAT Assessment 171
   (Includes proposer comment in Appendix A & B) 188

Task Force comments 208

Proposer response to Task Force comments 215

Final QIAT Assessment 216
Faster Payments Task Force Proposal

PayThat Payment System

April 30, 2016

Submitted by:

Stephen Lange Ranzini, President & CEO, University Bank, Ann Arbor, Michigan

+1(734) 741-5858 xt 9226 [desk]
+1(734) 741-5859 [fax]
ranzini@university-bank.com [email]
CONTENTS

Background ..................................................................................................................................... 4

Purpose of the Template and Instructions for Use ........................................................................ 5

Proposal Review Process ............................................................................................................. 6

Instructions for Submission and Proposal Review Process Timeline ......................................... 6

Legal Considerations ................................................................................................................... 7

Proposal Template ........................................................................................................................ 9

Executive Summary ........................................................................................................................ 9

Use Case Coverage ....................................................................................................................... 17

Supported Use Case Coverage Summary .................................................................................. 17

Cross-border Use Case Coverage (If Applicable) ...................................................................... 20

Proposal Assumptions (Optional) ............................................................................................. 21

Part A: Detailed End-to-End Payments Flow Description ........................................................... 23

Part A, Section 1: Solution Description .................................................................................... 23

1. Initiation .................................................................................................................................. 24

2. Authentication ...................................................................................................................... 32

3. Payer Authorization ............................................................................................................. 34

4. Approval by the Payer’s Provider ....................................................................................... 36

5. Clearing ............................................................................................................................... 38

6. Receipt .................................................................................................................................. 40

7. Settlement ............................................................................................................................ 44

8. Reconciliation ...................................................................................................................... 45

Part A, Section 2: Use Case Description ................................................................................... 51

Part A, Section 3: Use Case by Effectiveness Criteria ................................................................ 69

Part B: Business Considerations ................................................................................................... 72

1. Implementation Timeline ....................................................................................................... 72

2. Value Proposition and Competition .................................................................................. 74

3. Integration Effort ................................................................................................................ 120

Part C: Self-Assessment Against Effectiveness Criteria ............................................................ 124
1. Ubiquity .................................................................................................................... 125
2. Efficiency .................................................................................................................. 130
3. Safety and Security ................................................................................................... 133
4. Speed (Fast) .............................................................................................................. 143
5. Legal Framework ..................................................................................................... 146
6. Governance ............................................................................................................. 152
BACKGROUND

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

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

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

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

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

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

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

---

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

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

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

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

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

---

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

- Components include any of the following:
  - Rules, standards/protocols, and procedures
  - Physical or technical infrastructure, networks, systems and other resources needed by all parties to use or enable the rules, standards/protocols and procedures
  - Centralized or shared services, if any
  - Legal framework and enforcement mechanisms

- Parties include any of the following:
  - Governing bodies, operators, depository institutions, non-bank account providers and third-party service providers”.
Proposal Review Process

Once a proposal has been submitted, a qualitative assessment of the proposal against the Effectiveness Criteria will be conducted by the QIAT. During the assessment process, the proposer will have the opportunity to provide additional information and/or a response to the assessment. The proposer may also choose to withdraw its proposal at any point in during this initial assessment meaning that the proposal will not be shared with the Faster Payments or Secure Payments Task Forces. No confidential or proprietary information should be shared in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report.

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

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

Instructions for Submission and Proposal Review Process Timeline

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

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

Instructions providing details on where proposals are to be submitted will be provided in a separate communication prior to the submission window opening on April 1.
The following table outlines the proposal assessment process and timeline. Key dates for proposers are indicated in bold type.

<table>
<thead>
<tr>
<th>Timeline and key dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Proposers to submit proposals</td>
</tr>
<tr>
<td>2. Draft 1 of QIAT assessment and discovery period between QIAT and proposers</td>
</tr>
<tr>
<td>3. Proposers to provide written response to QIAT assessment or notification of decision to withdraw</td>
</tr>
<tr>
<td>4. Task Force review of proposal assessments commentary period</td>
</tr>
<tr>
<td>5. Proposer to submit final revised proposal, and written response to Task Force comments or notification of decision to withdraw prior to public release</td>
</tr>
<tr>
<td>6. Final QIAT assessment provided to proposers</td>
</tr>
<tr>
<td>7. QIAT report of all fully assessed proposals including Task Force commentary and proposer responses</td>
</tr>
</tbody>
</table>

**Legal Considerations**

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

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

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

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

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

EXECUTIVE SUMMARY

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

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

THE PAYTHAT PAYMENT SYSTEM EXECUTIVE SUMMARY

The PayThat Payment System is a bank-centric, true peer-to-peer, irrepudiatable, payment system that uses any email and text message based application platform to settle transactions and transmit associated transaction data securely even over an insecure network such as the Internet. PayThat can be used for transactions as small as fractions of a penny or as large as any amount.

Optionally, PayThat integrates payments data with XML-based transaction detail that interfaces with all standard eBilling & corporate ERP systems, enabling true eBilling automation.

PayThat uses open standard APIs that incorporate Persistent Digital Security to enhance privacy and to secure payments and transaction detail. PayThat uses state-of-the-art authentication methods and is capable of incorporating new methods, as they become available. It is device agonistic, covering all major platforms.

PayThat is modeled and documented using International Standards, such as the Unified Software Development Process and the Unified Modeling Language (UML). PayThat is compatible with all ISO Financial Services Technology Standards.

PayThat uses a cash purse system enhanced with end to end encryption of data at motion and at rest. During transactions good funds are push payments pushed from user to user. Adoption use cases have been developed that will drive rapid adoption of PayThat nationwide.

PayThat uses a superior “Data-Centric” approach to encryption and a “network of networks” architectural approach leveraging XML and XML tagged data pushed to edge servers from legacy applications, extending the usefulness of legacy applications and dramatically lowering cost of adoption for innovative solutions. The architecture methods of PayThat enable the following positive attributes as opposed to the negative attributes of the legacy payment systems and other emerging innovative solutions now deployed in the United States:
Positive Attributes

Consumer / Business Adoption Attributes
1. Something as easy as email; integrates with and has the look and feel of standard legacy email and SMS text messaging networks
2. Intuitive and easy to use & adopt
3. Solution uses a customer-friendly user interface
4. The functionality of the user interface can be scaled and automated; the same user interface can be simple or complex
5. Leverages methods that are ubiquitous and universal
6. Platform/device independent & agnostic
7. Infrastructure or equipment changes are as small as possible;
8. Has a good intuitive natural speech based brand
9. Voice based transaction capability is a plus
10. Leverages FSTC’s FAST interoperability authentication process leveraging existing Depository Institution internet and mobile banking security systems
11. Facilitates the development of an ecosystem of synergistic value added services such as Apps
12. Supports a directory of aliases so that email addresses and cell phone numbers do not need to be shared
13. Supports help wizards for consumer adoption support and ERP help wizards for business transaction support
14. Supports individuals who have multiple roles and delegations of authority

Negative Attributes

1. Requires participants to learn new system(s)
2. Adoption requires training & effort
3. Adoption requires training & effort
4. Different kind of participants must adopt and use different user interfaces
5. Requires participants to use additional system(s)
6. Limited to certain devices only or devices that have less than a large market share or does not support legacy devices
7. Requires new devices or infrastructure to be rolled out
8. Does not use a good brand or requires substantial investment to create a new brand
9. Does not support voice initiated transactions
10. Does not support interoperability with existing internet banking or mobile banking based authentication methods and processes
11. The network is closed and proprietary and to add synergistic services is a difficult effort
12. To complete a transaction email addresses or cell phone numbers or bank account numbers must be shared
13. Does not support help wizards
14. Does not support delegations of authority (e.g. aged parents, minor children guardians, business role)
15. Supports customer service models based on customer profitability

16. Supports the full range of payments from micro-payments to large payments

17. Solution enhances the privacy of personal data and discourages identity theft

18. Solution supports self-distribution via super distribution

19. Inexpensive to use, cheaper than existing alternatives by at least an order of magnitude (10x)

20. Installation and adoption is easy

**Security & Privacy Attributes**

21. Secure way to send money and associated data over insecure networks

22. Supports encryption of all data end to end and at rest (a/k/a Persistent Digital Security)

23. Data is never "in the clear"

24. Supports multiple state of the art methods

25. Supports encryption methods whose algorithms are secure and vetted in a public ANSI/ISO process

26. Supports new methods as they become available

27. Voice based transaction security is a plus

28. Supports "Strong Authentication": a physical trait combined with a personal

authority variations)

15. Cannot differentiate customer support by customer profitability

16. Systems & networks are "balkanized" and add additional niche payment networks for market adoption slices

17. Solution continues to value PII data to validate transactions that can be stolen from individuals and businesses, encouraging more identity theft

18. Solution must be sold for consumers and businesses to adopt; usage and adoption is not encouraged or easy for new users

19. Solution is comparably priced to existing legacy Solutions

20. Installation process is time consuming or cumbersome

21. Requires more expensive secure networks to securely send money and associated data

22. Encryption support is not end to end and/or at rest

23. Data is decrypted even for a moment or in one process

24. Supports or requires non-standard or proprietary technologies, or just one methodology

25. Supports or requires non-standard or proprietary encryption technologies

26. Is architecturally rigid

27. Does not support voice based transaction authentication

28. Uses shared secrets (passwords, mother's maiden name, SSN, first
possession

29. Does not use personal information for authentication, the use of which only encourages identity theft
30. Security can be scaled as needed, and increased in real-time as transaction risk requires
31. Supports authentication of Trusted Platform Module chips embedded in devices
32. All users are strongly enrolled and strongly authenticated using I-9 documents
33. Outsources investigation of wrongdoing to a law enforcement agency that will actually investigate wrongdoing
34. "Keys" that enable the movement of money, are encrypted at all times
35. "Keys" that enable the movement of money are shared only as necessary to complete a transaction
36. The weakest node of the network is very secure and robust against penetration or compromise
37. Solution is decentralized
38. Solution uses a “Data-Centric” approach to encryption: data access is controlled by role & authority on a transaction level basis; access controlled by users at the nodes
39. Access to all data is controlled by rules enforced by strong encryption, providing greater control & security
40. Data is persistently secured and encrypted, so that data can travel freely across the cloud, databases or insecure systems/networks as an encrypted, secure data element and still be teacher's name) that cannot be the basis for "Strong Authentication"
29. Requires use of personal information (passwords, mother's maiden name, SSN, first teacher's name) in any part of the authentication process
30. One size fits all security for all transactions, transaction types and participants
31. Does not support Trusted Platform Module device authentication
32. Identity is not proofed person to person or using I-9 government documents
33. Requires in-house legal enforcement or referrals to law enforcement agencies that will not investigate small wrongdoing
34. "Keys" that enable the movement of money, such as account numbers, are accessible at multiple points during the transaction life cycle
35. "Keys" that move money, such as account numbers, are accessible to many parties during the transaction life cycle
36. The security of a network is only as good as its weakest node and the weakest node is vulnerable to compromise
37. Solution requires centralized databases with large value, a large cyber security target
38. Solution administrator(s) have access to the keys to decrypt and access any information. Enables greater theft of data since 70% of all data breaches are by insiders.
39. Data is not protected by persistent rules based access requirements that are enforced by strong encryption
40. Data is "in the clear" or can be extracted and made to be "in the clear"
access controlled based on role and authority

41. Access to data is not controlled or the control is not granular or based solely on need to know and for the duration required

42. Merchants collect and store all data

43. Control of data is by database administrators, relies on good faith of administrators, or cannot be fine-tuned by industry ecosystem needs

Content

44. Supports transmission of secure payments only but not associated transaction data or uses inflexible mainframe based legacy standards such as X12

45. Does not support XML or ISO 20022 standards

46. Does not support data interfaces with standard ERP systems and bank web billing systems or does not support STP

47. Supports or requires only non-standard or proprietary APIs

Governance

48. Does not support a recognized IdM governance framework and a new rules system must be developed, over a lengthy timeframe

49. User agreements including data ownership rules and data access rules are set by network and forced on consumers or negotiated bi-laterally

50. Does not support automation of escheat laws

51. Supports only certified & registered funds (similar to bank deposits)
52. Supports data anonymized econometric research process for the Federal Reserve System
53. Supports law enforcement research process to support real-time AML and anti-terrorism
54. Solution itself requires and facilitates compliance with privacy laws & regulations (GLB, AML, BSA, HIPAA, FACTA)
55. Rules based controls provide enhanced security, quality assurance and audit trail

**Depository Institution Industry Adoption**
56. The PayThat Payment System holds stored value in the form of good funds within blocked bank deposits for funds deposited into the payment network and supports push payments only; legacy business models utilizing debit pull today can be fully supported in a good funds environment with revocable prior authorization automation by participants that then lead to push payments.
57. Solution allows funds to flow easily between the new Solution and the legacy bank centric payment systems
58. Solution has a defined role for larger banks to serve as clearing or correspondent banks for smaller Depository Institutions
59. Solution supports automation of non-repudiation of transactions
60. Solution leverages Gresham's law: charge nothing to take money in; charge to take money out
61. Solution leverages Metcalfe's law: Solution can support multiple use cases and value added services
62. Solution leverages email backbone for easier implementation and adoption

52. Does not support data analysis for econometric research
53. Does not support law enforcement research process
54. Solution requires additional expense & overhead to ensure compliance with privacy laws & regulations
55. Controls to ensure security, quality assurance or audit are manual or rely on dual control
56. Supports debit pull or adds transaction settlement finality risk
57. Solution is a walled garden or only partially interoperable with one or more legacy payment systems
58. Solution ensures large bank market share loss
59. Solution requires a large set of rules to govern transaction finality
60. Solution has undefined economic incentives for adoption and retention of the stored value blocked funds in the network
61. Solution does not have a dynamic where the value increases based on number of users and functionalities of the network
62. Solution requires firewall and system modifications for adoption by business and consumers
63. Solution can be run over insecure, partially secure or very secure sigma six reliable networks depending upon use cases & needs

63. Requires more expensive secure networks to securely send money and associated data depending upon use cases & needs

What is PayThat?

- A Persistent Digital Security (PDS) based cash purse (CashBox)
- A GUI software utility that interfaces with any standard email browser (CashBox)
- Sends email or text messages with a file attachment
- The file attachment is PDS based
  - A .pay file
  - Uses cryptographic standards that make an attack uneconomic in both the length of time to crack a file and the cost versus benefit to the attacker.
  - The .pay file uses cryptographic standards so that each data element is separately encrypted such that data elements are accessible solely and variably based on role, authority, authentication status and need to know.

Advantages of PayThat

- Uses email or text messaging for transmission
- Ubiquitous & universal
  - Intuitive and easy to use & adopt
  - Integrates with and has the look and feel of standard legacy email and SMS text messaging software and networks
- Platform/device independent & agnostic (PC, Mobile Device, Legacy Systems & etc.)
- Security Agnostic
  - Sender chooses authentication method
  - Could use any security method that is supported by the Solution
- Completely Scalable
  - Micro-payments
  - P2P (consumer to consumer)
  - B2C (business to consumer)
  - B2B (business to business)
  - G2P (government to consumer)
  - G2B (government to business)
  - G2G (government to government)
- Enhances privacy of Personally Identifiable Information
Payments and payment instructions can optionally be sent securely across the wild internet, a completely insecure network, where a transaction cost is then zero

- Self-distribution via superdistribution
- Consumer controlled rules based access provides greater control & security
- Links to existing bank payment systems through “Clearing Banks” that manage an internet bank payments gateway
- Instant payment; optionally, same day settlement to or from legacy banking system
- Non-repudiation of payments
- Inexpensive to use
- Optional integration to consumer eBilling & corporate B2B ERP systems
- By using a “network of networks” architectural approach leveraging XML, XML tagged data pushed to edge servers from legacy applications, mapping & interoperability standards, interoperability among legacy infrastructures such as legacy bank platforms and bank payment systems can be ensured, extending their usefulness and dramatically lowering cost of adoption for innovative solutions
- By using a “Data-Centric” approach to encryption where data access is controlled by role & authority on a transaction level basis, access to all data is controlled by users at the nodes with access controlled by rules enforced by strong encryption, providing greater control & security.
- Access is controlled by role, authority, need to know and only for the duration that it is needed to be known
- Data is persistently secured and encrypted, so that data can travel freely across the cloud between edge servers, databases or insecure systems/networks as an encrypted, secure data element and still be access controlled based on role and authority
- Data can be ubiquitous & access controlled. Data access is controlled only by users, utilizing standard privacy templates by ecosystem
- Processing of XML data can be accelerated if needed by using XML compilers
PayThat Solution Message Flow

PayThat Solution Message Flow & Elements

Depository Institution 1 (FI-1)

Depository Institution 2 (FI-2)

Participant 1 (S-1)

Participant 2 (S-2)

Legacy Payments Network

Legacy Payments Network

B2B EXCHANGE (Optional)

USE CASE COVERAGE

Supported Use Case Coverage Summary

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

© 2016 Federal Reserve Banks & University Bank. Materials are not to be used without consent.
<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>N</td>
<td>The solution assists business and governments to make payments. Payments supported include: social security, government pensions and employee wages.</td>
<td>Note that the solution targets regular income payments to individuals. It would not be suitable for all types of business-to-person payments, such as ad hoc legal settlement payments or medical insurance claims.</td>
</tr>
<tr>
<td>Business to Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported. Transaction data interchange is optionally fully supported to automate STP and ERP integration. Example payments supported: (ad hoc low value) Just-in-time supplier payments, supply chain e-invoicing, Cross Border Single Window Trade Facilitation payments and data exchange, Health Information Exchange related payments</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported including ad hoc low value and ad hoc high value. Example payments supported: Wages for temporary workers or time sensitive corrected payroll (ad hoc low value), Medical insurance claims, legal settlements, FEMA transfers (ad hoc high value)</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
</tbody>
</table>
## Supported use case coverage summary

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td><em>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported. Example payments supported:</em> emergency bill payment, time-sensitive corrected bill payment, media and web services related micropayments, First Class Email related micropayments, Health Information Exchange related payments</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td><em>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported. Example payments supported:</em> paying a friend or micro business, First Class Email related micropayments</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
</tbody>
</table>
Cross-border Use Case Coverage (If Applicable)

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

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>Via CHIPS and correspondent depository institution accounts in each country the local ACH and RTGS (wire) payments systems can be accessed to settle transactions with local legacy payment systems. The banks in each country will desire to participate in the solution by establishing one or more PayThat Payment System Clearing Banks covering their country’s legacy payment systems.</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems. The global payment gateway has been architected but is not yet built.</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Via CHIPS and correspondent depository institution accounts in each country the local ACH and RTGS (wire) payments systems can be accessed to settle transactions with local legacy payment systems. The banks in each country will desire to participate in the solution by establishing one or more PayThat Clearing Banks covering their country’s legacy payment systems.</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems. The global payment gateway has been architected but is not yet built.</td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Via CHIPS and correspondent depository institution accounts in each country the local ACH and RTGS (wire) payments systems can be accessed to settle transactions with local legacy payment systems. The banks in each country will desire to participate in the solution by establishing one or more PayThat Clearing Banks covering their country’s legacy payment systems.</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems. The global payment gateway has been architected but is not yet built.</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Via CHIPS and correspondent depository institution accounts in each country the local payments systems can be accessed to settle transactions. The banks in each country will desire to participate in the solution by establishing one or more PayThat Clearing Banks covering their country’s legacy systems.</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems. The global payment gateway has been architected but is not yet built.</td>
</tr>
</tbody>
</table>
Proposal Assumptions (Optional)

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

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

Within six months of the commencement of initial work to build PayThat, an intellectual property search by a nationally recognized law firm specializing in intellectual property will be performed to determine a strategy to resolve or manage, prior to implementation, any legal, operational or financial risks to the Payment System, End Users and Providers arising from third-party intellectual property rights (including patents, trademarks, copyrights and trade secrets). To date, University Bank has only undertaken a partial due diligence investigation of potentially applicable intellectual property rights to the PayThat proposal, with the result that the patents listed in this section have been identified. A significant amount of University Bank owned intellectual property has been incorporated into this copyrighted document.

1. University Bank establishes a special purpose entity (PayThat Corporation) to acquire the intellectual property rights, licenses and/or patents and business vendor relationships required (as described in this section) to build the Solution, and the Solution is able to obtain the funds to build the Solution.
2. The domain names paythat.com, paythat.net, paythat.org, IdentityAssuranceFederation.com, IdentityAssuranceFederation.net and IdentityAssuranceFederation.org can be purchased by PayThat Corporation from Jove Corporation, a corporation under common control by the controlling shareholders of University Bank.
3. The domain names currency-exchange.com and currency-exchange.net can be purchased by PayThat Corporation from University Bank.
4. PayThat Corporation can acquire licenses and/or ownership of key internet security related patents held by Jove Corporation, a corporation under common control by the controlling shareholders of University Bank.

5. PayThat Corporation can license and/or acquire key encryption patents held by TecSec, an entity controlled by Ed Scheidt.

6. PayThat Corporation can enter into a vendor relationship with TecSec, an entity controlled by Ed Scheidt, to obtain access to utilize the .post top level domain for its enrollment and identity proofing operations, as described in Part A, Section 1, Paragraph 1 (Initiation).

7. SEMHIE/MiHIN agrees to serve as a pilot customer for the proposed healthcare payment automation and Identity Assurance Federation services.

8. PayThat is able to license United States Patent #5,999,967, “Electronic mail filtering by electronic stamp”, owned by Todd Sundsted to be able to launch the First Class Email use case described in this proposal.
Part A: Detailed End-to-End Payments Flow Description

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

Part A, Section 1: Solution Description

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

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

Proposers should include flow diagrams of the messaging and payment flows and the roles of stakeholders (end users, technology providers, processors, including the proposer(s) of the solution) through the eight lifecycle stages of the solution. In completing this section, proposers

---

3 Definitions of some of the terms used below are either defined in the Effectiveness Criteria or in the Glossary of Terms.
should refer to the Effectiveness Criteria that relate to each of the eight stages (as noted in the instructions for each sub-section).

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

1. **Initiation**

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

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

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

**Initiation Overview**

A Consumer or End-User may either learn about the benefits of the PayThat Payment System and opt to enroll in PayThat or receive a .pay file that actually has good funds in it from a friend or business associate via email or text message and opt to enroll in PayThat to deposit the funds in a PayThat CashBox.

**a. Enrollment**

An End-User will only be allowed to download the PayThat software application and use the service to transmit funds following strong enrollment and strong authentication. What is "strong authentication"? This combines a physical trait – a biometric such as a voiceprint or fingerprint, captured during the strong enrollment process – with a personal...
possession, such as a smart phone, which is strongly enrolled and strongly authenticated, using the device’s Trusted Platform Module (TPM) chip and Automatic Number Identification (ANI). The TPM chip contains an Asymmetric Cryptographic Key Pair, one private and one public, which securely identifies a device. Other devices such as a tablet, laptop and desktop can be similarly strongly authenticated.

Strong enrollment is a foundational piece to everything that follows. The enrollment process of PayThat will incorporate the following foundational principles:

1. The level of assurance of identity proofing will rise from Level 1 to Level 4 per the NIST 800-63-2 standard based on risk and the dollar size of a proposed transaction:
   a. Level 1 enrollment (self asserted identity) would only allow an End-User to register for the PayThat service and learn more about it, including the fee schedule;
   b. Level 2 enrollment will be required to open a PayThat account or to deposit the funds from a .pay file received by an End-User from a Level 3 or Level 4 PayThat enrolled End-User into a CashBox;
   c. Level 3 enrollment will be the minimum requirement to actually initiate a transaction to pay another End-User or to withdraw money from a CashBox; Participants with high risk may not be allowed to complete enrollment based on the PayThat Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) policy, and all End-Users banned from the banking system as a result of OFAC regulations shall not be allowed to complete enrollment.
   d. Level 4 enrollment (in person identity proofing using the I-9 standard and NIST 800-63-2) will be required if an End-User wants to initiate a transaction greater than a set dollar amount as established by the PayThat Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) policy. Level 4 enrollment will be the minimum requirement to actually initiate a transaction to pay another End-User deemed by PayThat Payment System BSA/AML Rules to be medium or high risk.

2. End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers, or prohibited transactions, such as a gambling transaction prohibited by Regulation GG). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices.

3. The following methods will be supported:
   a. Asymmetric Cryptographic Key Pairs, one private and one public. Keys get generated and credentials get bound to the End-User Identity Record and to a
device that has been strongly authenticated and strongly enrolled as linked to the End-User.
b. Bio-metric combined for two-factor authentication for NIST 800-63, Level 3 or Level 4 of assurance. The credentials get bound to the End-User Identity Record.
c. One time Passwords using Out of Bound (OOB) transmitted to a device that has been strongly authenticated and strongly enrolled as linked to the End-User.
d. Single-sign on (SSO) using existing Depository Institution mobile banking or internet banking services login authentication via a device that has been strongly authenticated and strongly enrolled as linked to the End-User.
Ongoing authentication of the End-User and device(s) is performed using "information assurance" methods (making sure that whatever device the user connects from is safe enough to ensure that the transactions have really been authorized by the legitimate End-User).
If enrollment isn't performed well, there isn't much basis for trusting any transaction that follows.
4. Accurate identification of an individual prior to allowing them to transact with merchants and financial institutions. PII will not be used to authenticate transactions once an End-User is strongly enrolled. The PayThat payment system will accumulate PII data in an encrypted database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only. This database will be the foundation for an identity management service called the Identity Assurance Federation (IAF). Done properly, this will eliminate the identity theft ecosystem and greatly reduce identity theft. The IAF enables a valuable value added service, a credit bureau owned by Depository Institutions, the subject of a separate proposal. The IAF has an estimated value of $10 billion and can generate $1 billion per year in net income. Additional details on the IAF can be provided to an interested party under the terms of University Bank’s standard Mutual Non-Disclosure Agreement (MNDA).
5. "Shared secrets" that can be stolen, intercepted and shared (like a mother's maiden name, password, user id or where you went to elementary school) cannot be the basis for strong enrollment or strong authentication. This will devalue PII since it would not be able to be used to steal money from the PayThat Payment System and if PayThat becomes ubiquitous over time, this would undermine the fundamental business case for the identity theft ecosystem, since identity theft would no longer be profitable and greatly reduce identity theft.
6. Level 3 and Level 4 enrollment will utilize as a part of the process a web service that creates an email account with a .post.us top level domain. This has the result that any identity related fraud will be investigated by the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal Service. Also, through an existing treaty through the Universal Postal Union (UPU), any attempted or actual identity fraud in any of 190 member countries of the UPU, each of which have their own Postal Inspection Service law enforcement agency, is capable of being
investigated by that country’s Postal Inspection Service law enforcement agency. Unlike the FBI, which has a $500,000 limit on financial fraud before they will investigate, the U.S. Postal Inspection Service investigates every reported fraud or attempted fraud incident. Therefore, at the cost of a small fee, investigations of fraud or attempted fraud can be outsourced by PayThat to existing federal and international law enforcement agencies. Additional details on the .post.us business model can be provided to an interested party under the terms of University Bank’s standard Mutual Non-Disclosure Agreement (MNDA).

7. At enrollment, participants selected a privacy template level of high, medium or low. These privacy templates can be fine tuned to the specific needs of industry ecosystems, e.g. healthcare for HIPAA requirements. In the privacy template users can mandate who has access to data by role and authority. With a high privacy template setting a degree of anonymity can be assured for participants. Merchants may incentivize participants to select a low or medium privacy template to enroll in additional value added services, such as loyalty point programs. End-users may obtain a report detailing the data collected about them under the terms of the privacy template they adopted as modified from time to time.

8. Authentication methods will evolve over time based on the evolving threat landscape.

Because the PayThat Payment System is device agnostic provided that the device is reasonably secure, vision or hearing impaired individuals, individuals with other disabilities, the elderly and individuals with limited English proficiency will be able to use their existing devices and assistive methods that they use currently to access internet, cell phone or web services, ensuring widespread usability. In addition, the CashBox utilizes a GUI menu that is very simple with few options, however by turning on additional optional services and menu options, a user can access higher levels of complexity in using PayThat, if desired. Participants will therefore have the ability to use PayThat at the level of technological proficiency that they themselves desire.

End-Users may opt to use one, two or more PayThat Clearing Banks and may freely change with whom they do business. During the initial enrollment process PayThat Clearing Banks are required to fully disclose all fees, terms and conditions applicable to their PayThat account.

b. Initiation

Once enrolled and the PayThat software is installed on the device(s) selected by an End-User, they may load value in their CashBox and then initiate transactions using PayThat.

1. Participant loads value into the CashBox. Participants can load value into the CashBox in two ways, by depositing the funds from a .pay file received by the participant from a Level 3 or Level 4 PayThat participant, or by registering or signing up for a PayThat account with either their own Depository Institution, if it supports PayThat, or by choosing a PayThat
enabled Depository Institution from a list provided during the sign-up process and then funding that account. Accounts can be funded:

a. From an existing Depository Institution account by initiating an electronic transfer, via ACH, wire, credit or debit card, internal transfer between depository accounts at their Depository Institution, draw on available electronic line of credit & etc. Access to these accounts can be facilitated through SSO accessing the participants existing online banking or mobile banking services.

b. By depositing the funds from a .pay file received by the participant from a Level 3 or Level 4 PayThat participant.

c. By depositing funds via an MSB and/or merchant that supports PayThat loading via cash or check.

When good funds are loaded into a CashBox, they are present in the ledger of the Depository Institutions’ Fed Funds account and virtually present in the CashBox in the form of PayThat Tokens. PayThat tokens are cryptographic artifacts that can be denominated in any currency or optionally in a virtual currency such as BitCoin, or a combination of a virtual currency and a fiat currency such as Dollars.

The following diagram indicates the message flow for initiation of a transaction:
2. Participant selects an amount and a payee using the PayThat software. Payees can be any email address, cell phone number or alias (aliases are listed in the CIF Database and optionally broadcast on a variable basis based on the participants privacy templates where participants can mandate who has access to their data by role and authority).
   a. When the participant confirms the amount and payee and either manually or by voice says “Pay That”, Message #1, Send Money Notification is sent as a blind carbon copy (bcc) not readily visible to the participant to the participant’s Depository Institution’s PayThat Clearing Bank (FI-1), so that it can be alert the recipient’s Depository Institution, if the payee is not a customer of FI-1, and to be ready to clear the transfer if it is between two customers of FI-1. FI-1 places a record of the pending transaction in the Pending Transactions database.
b. If the payee is not a customer of FI-1, **Message #2** Send Money Notification is sent to the payee’s Depository Institution’s PayThat Clearing Bank (FI-2), so that it can be ready to clear the transfer if the payee instructs it to deposit the funds and clear the transaction.

c. If the payee is not a customer of FI-1, **Message #3** Confirm Receipt of Send Money Notification is sent by FI-2 to FI-1, to ensure Message #2 was correctly received. Upon transmission of Message #3, good funds are transferred from FI-1’s ledger to FI-2. Actual settlement may be real-time or batch, as established by prior agreement of the two Depository Institutions. For example, they may agree to hold and aggregate all transactions until the FDIC insurance limit of $250,000 is reached, or a lesser amount of $200,000 to provide an extra margin of safety. Per the prior agreement of the Depository Institutions, this settlement may either be via ACH and/or FedWire exchanged between the actual Depository Institutions themselves. Actual settlement occurs only after Message #6 is received and validated (see below).

d. Upon receipt of Message #1 or alternatively if Message #2 was sent, upon the receipt of Message #3, **Message #4** is sent to the participants PayThat CashBox to confirm receipt of Message #1.

e. Upon receipt of Message #4, **Message #5** Send Money Notification is sent to the payee (Participant 2 or S-2) via the method selected either email or text message. If an alias is used, the message is sent via the method selected by Participant 2 in the alias they established.

f. To open the .pay file and access its contents including the money contained in it, S-2 must be an enrolled PayThat participant and authenticate themselves to the IAF (the Authentication Server) or log in to their Depository Institution’s participants existing online banking or mobile banking services. If S-2 is not an enrolled PayThat participant, they will receive a marketing message encouraging them to sign up and enroll in the PayThat Payment System to access the funds in the .pay file. This viral marketing technique is a form of super distribution. If S-2 opts to deposit the money contained in the .pay file into their CashBox, **Message #6** Deposit Money Notification is sent to FI-1, if S-2 is a customer of FI-1, or to FI-2, per the diagram. Upon receipt of Message #6, FI-2 (or FI-1 if FI-1 received this message) confirms that an identical request is present in the Pending Transactions Database and the transaction clearing process is completed (see Message #3, above.

g. If Message #6 was sent to FI-1 or FI-2, and the validity of Message #6 is confirmed by consulting the Pending Transactions Database, **Message #7** Confirm Deposit Money Notification is sent to S-2, to ensure S-2 that Message #6 was received and to facilitate the clearing process with S-1’s CashBox.

h. Upon receipt of Message #7 by FI-1 or FI-2, FI-1 or FI-2 sends **Message #8** Confirm Deposit Money Notification is sent to S-1, and S-1’s CashBox moves the transaction from pending to complete, so the participant knows and has proof that
the funds were transmitted to S-2 per their instructions and cleared by their Depository Institution(s).

Participants are not allowed by the PayThat CashBox to initiate a transaction for more good funds than are already present in their CashBox. If Participant has a desire to send good funds for a larger amount, they must load additional good funds into their CashBox (see Section 1 Participant loads value into the CashBox above). Overdrafts are never allowed and overdraft fees are never incurred in the PayThat Payment System. The CashBox provides participants with a current correct total of good funds available for initiation of transactions at all times. Participants can optionally delegate the CashBox to automatically load good funds into the CashBox based on the prioritization of preferred methods, using the methods outlined in Section 1 Participant loads value into the CashBox above. For example, a participant may want to refresh additional funds into their CashBox when the balance of good funds drops under $250 in increments of $100. Any amounts for such automated reloading of good funds can be selected.

Participants can optionally delegate the CashBox to automatically approve, or as a further option an approval upon confirmation by the End-User, requests for payments by recurring billing businesses. This combined with the automated reloading of good funds can ensure transactions are cleared if the End-User wants them to clear and has the funds available in any of:

a. the End-User’s CashBox;

b. the End-User’s linked deposit accounts at their Depository Institution(s); and

c. End-User’s linked credit/line of credit accounts at their Depository Institution(s).

In this manner the current business model involving Pull Payments for businesses that bill End-Users monthly can be supported by the PayThat Payment System, however using a good funds model that avoids overdrafts and overdraft fees. End-Users would be alerted in real-time if insufficient funds are available in the linked accounts to pay a requested transaction so that they can take further action (e.g. request and obtain a short term loan from their Depository Institution.

The PayThat Payment System can optionally be run in “bearer funds” mode where transactions occur only bi-laterally between S-1 and S-2 and are not cleared through FI-1 or FI-2 by S-2. In this mode, S-2 takes the full risk of loss of the PayThat Tokens if S-2’s device suffers a failure and the PayThat software on S-2’s device is not fully backed up. Such transactions can offer a full replacement for cash, coins and currency. The PayThat Payment System could impose system constraints that require clearing through FI-1 and/or FI-2, depending upon the use case, for all amounts above a system preset dollar limit, or a cumulative amount of transactions above a certain system preset dollar limit.

All of the many use cases and optional use cases have been fully mapped in Unified Modeling Language (UML) and are available under a Mutual Non-Disclosure Agreement (MNDA) for review.
2. **Authentication**

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

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

Strong authentication is critical for all transactions. If authentication isn't performed well in each case, there isn't much basis for trusting any transaction that follows. The PayThat authentication process, which is mandatory for all End-Users prior to accessing a CashBox, is accessed by the End-User through the PayThat software via one of two methods:

A. Single-sign on (SSO) using End-User’s existing Depository Institution mobile banking or internet banking services login authentication via a device that has been strongly authenticated and strongly enrolled as linked to the End-User; and

B. Direct sign-on using the authentication process of the identity management service called the Identity Assurance Federation (IAF).

The authentication process of PayThat will incorporate the following foundational principles:

1. The level of assurance of identity proofing will rise from Level 1 to Level 4 per the NIST 800-63-2 standard based on risk and the dollar size of a proposed transaction:
   e. Level 1 enrollment (self asserted identity) would only allow an End-User to register for the PayThat service and learn more about it, including the fee schedule;
   f. Level 2 enrollment will be required to open a PayThat account or to deposit the funds from a .pay file received by an End-User from a Level 3 or Level 4 PayThat enrolled End-User into a CashBox;
   g. Level 3 enrollment will be the minimum requirement to actually initiate a transaction to pay another End-User or to withdraw money from a CashBox;
   h. Level 4 enrollment (in person identity proofing using the I-9 standard and NIST 800-63-2) will be required if an End-User wants to initiate a transaction greater than a set dollar amount as established by the PayThat Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) policy. Level 4 enrollment will be the minimum requirement to actually initiate a transaction to pay another End-User deemed by PayThat Payment System BSA/AML Rules to be medium or high risk.

2. End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single
solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices.

3. The following methods will be supported:
   a. Asymmetric Cryptographic Key Pairs, one private and one public. Keys get generated and credentials get bound to the End-User Identity Record and to a device that has been strongly authenticated and strongly enrolled as linked to the End-User.
   b. Bio-metric combined for two-factor authentication for NIST 800-63, Level 3 or Level 4 of assurance. The credentials get bound to the End-User Identity Record.
   c. One time Passwords using Out of Bound (OOB) transmitted to a device that has been strongly authenticated and strongly enrolled as linked to the End-User.
   d. Single-sign on (SSO) using existing Depository Institution mobile banking or internet banking services login authentication via a device that has been strongly authenticated and strongly enrolled as linked to the End-User.
   e. Ongoing authentication of the End-User and device(s) is also performed using "information assurance" methods (making sure that whatever device the user connects from is safe enough to ensure that the transactions have really been authorized by the legitimate End-User).

4. Accurate identification of an individual is required prior to allowing them to transact with merchants and financial institutions. PII will not be used to authenticate transactions once an End-User is strongly enrolled. The IAF will accumulate PII data in a database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only. Done properly, this will eliminate the identity theft ecosystem and greatly reduce identity theft. The IAF enables a valuable value added service, a credit bureau owned by Depository Institutions, the subject of a separate proposal. The IAF has an estimated value of $10 billion and can generate $1 billion per year in net income. Additional details on the IAF can be provided to an interested party under the terms of University Bank’s standard Mutual Non-Disclosure Agreement (MNDA).

5. “Shared secrets” that can be stolen, intercepted and shared (like a mother's maiden name, password, user id or where you went to elementary school) cannot be the basis for strong enrollment or strong authentication. This will devalue PII since it would not be able to be used to steal money from the PayThat Payment System and if PayThat becomes ubiquitous over time, this would undermine the fundamental business case for the identity theft ecosystem, since identity theft would no longer be profitable and greatly reduce identity theft.

6. Level 3 and Level 4 authentication will utilize as a part of the process a web service that generates an email message with a .post.us top level domain from the Authentication Server to the IAF confirming authentication of the End-User. This has the result that any identity related fraud will be investigated by the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal
Service. Also, through an existing treaty through the Universal Postal Union (UPU), any attempted or actual identity fraud in any of 190 member countries of the UPU, each of which have their own Postal Inspection Service law enforcement agency. Unlike the FBI, which has a $500,000 limit on financial fraud before they will investigate, the U.S. Postal Inspection Service investigates every reported fraud or attempted fraud incident. Therefore, at the cost of a small fee, investigations of fraud or attempted fraud can be outsourced by PayThat to existing federal and international law enforcement agencies. Additional details on the .post.us business model can be provided to an interested party under the terms of University Bank’s standard Mutual Non-Disclosure Agreement (MNDA).

7. Authentication methods will evolve over time based on the evolving threat landscape.

8. Authentication should under normal circumstances take 30 seconds or less with an average participant (S-1 or S-2).

3. **Payer Authorization**

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

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

After Participant loads value into the CashBox (see **Participant loads value into the CashBox** above), the Participant may authorize one or more transactions. To authorize a transaction Participant must be in authenticated status (see **Authentication** above) because the CashBox cannot be accessed unless the Participant is authenticated. Participant then selects an amount and a payee using the PayThat software (see **Participant selects an amount and a payee using the PayThat software** above). The participant then confirms the amount and payee and either manually through a strongly enrolled and strongly authenticated device or by voice through a strongly enrolled and strongly authenticated device says “Pay That”, generating **Message #1** (see above), Send Money Notification to the participant’s Depository Institution’s PayThat Clearing Bank (FI-1), so that it can be alert the recipient’s Depository Institution, if the payee is not a customer of FI-1, and to be ready to clear the transfer if it is between two customers of FI-1. FI-1 places a record of the pending transaction in the Pending Transactions database.

Participants can optionally delegate the CashBox to automatically approve, or as a further option an approval upon confirmation by the End-User, requests for payments by recurring billing businesses. This combined with the automated reloading of good funds can ensure
transactions are cleared if the End-User wants them to clear and has the funds available in any of:

a. the End-User’s CashBox;
b. the End-User’s linked deposit accounts at their Depository Institution(s); and
c. End-User’s linked credit/line of credit accounts at their Depository Institution(s).

In this manner the current business model involving Pull Payments for businesses that bill End-Users monthly can be supported by the PayThat Payment System, however using a good funds model that avoids overdrafts and overdraft fees. End-Users would be alerted in real-time if insufficient funds are available in the linked accounts to pay a requested transaction so that they can take further action (e.g. request and obtain a short term loan from their Depository Institution. For each pre-authorized transaction the Participant can set defined parameters that limit the approved authority granted by the Participant. Parameters can include account from which funds are drawn, payee, frequency, time and date, amount, amount limits, duration of authorization, etc.). The set of pre-authorizations made by the Participant are fully visible to the Participant under the CashBox’s Pre-authorized and Pending Transactions Menu. While the Participant can change the parameters for all pre-authorized transactions in real-time in the CashBox, all other actions and alerts under this optional use case can occur in near real-time, the only limiting factor being the speed with which the actual email or text message based communication among the parties can occur.

All pending transactions are visible 24/7/365 in the Participant’s CashBox as pending authorized transactions. An End-User can revoke pre-authorization or change relevant parameters for pre-authorization at any time in real-time, prior to the actual agreed upon time that the good funds are pushed from the CashBox for the pre-authorized transaction authorized by the Participant.

In a corporate environment, two or more authorizations from two or more CashBoxes controlled by two or more Participants may be required to authorize a transaction, based on role and authority. In this way, dual control and approval based on hierarchies of authority can be enforced. This method can fully support e-billing, including generation of e-bills, payment of e-bills and generation and handling of e-invoicing data through the secure, encrypted at motion and at rest PayThat Payment System and the related CashBoxes controlled by corporate End-Users and participants.

In a consumer environment where guardianships (for elderly adults or minor children) or trustee relationships, or for married parties, two or more authorizations from two or more CashBoxes controlled by two or more Participants may be required to authorize a transaction. In this way, dual control and approval based on hierarchies of authority can be enforced. In this way, a fully competent adult can be a second approver for a less than fully competent individual, while still providing the less than fully competent individual a higher degree of financial autonomy. If required or desired, dual control can be established using two or more fully competent adults, the second of whom has “approval only” authority. This method can
reduce or even eliminate financial abuse of minor children, minimally competent adults and elder financial abuse.

While a typical PayThat transaction across the wild internet or native telco networks will have no cost, transactions that require Sigma 5 or Sigma 6 reliability may be routed across more expensive and more reliable networks. Any additional fees for additional optional services of any type will be fully disclosed and required consent of the Participant prior to completion of the Authorization process and release of any good funds by the CashBox.

All data in the CashBox and all communications between the CashBox and S-2, FI-1 and FI-2 are encrypted at motion and at rest, except for that data being entered by the Participant into the CashBox prior to it being encrypted and any data temporarily unlocked and being viewed in the CashBox by the Participant on their strongly enrolled and strongly authenticated device.

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

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

   a. To initiate a payment the Participant must gain access to the CashBox on the strongly authenticated and strongly enrolled device and Participant must be a strongly enrolled End-User, and must have strongly authenticated their identity to open the CashBox. When the participant confirms the amount and payee and either manually or by voice says “Pay That”, Message #1, Send Money Notification is sent as a blind carbon copy (bcc) not readily visible to the participant to the participant’s Depository Institution’s PayThat Clearing Bank (FI-1), so that it can be alert the recipient’s Depository Institution, if the payee is not a customer of FI-1, and to be ready to clear the transfer if it is between two

---

4 The completion of payment initiation is defined as just following payer authorization to their provider, or just following confirmation by the payer’s provider that pre-authorization exists for a given payment.
customers of FI-1. FI-1 places a record of the pending transaction in the Pending Transactions database.

b. If the payee is not a customer of FI-1, **Message #2 Send Money Notification** is sent to the payee’s Depository Institution’s PayThat Clearing Bank (FI-2), so that it can be ready to clear the transfer if the payee instructs it to deposit the funds and clear the transaction.

c. If the payee is not a customer of FI-1, **Message #3 Confirm Receipt of Send Money Notification** is sent by FI-2 to FI-1, to ensure Message #2 was correctly received. Upon transmission of Message #3, good funds are transferred from FI-1’s ledger to FI-2. Actual settlement may be real-time or batch, as established by prior agreement among the two Depository Institutions. For example, they may agree to hold and aggregate all transactions until the FDIC insurance limit of $250,000 is reached. Per the prior agreement of the Depository Institutions, this settlement may either be via ACH and/or FedWire exchanged between the actual Depository Institutions themselves. Actual settlement occurs only after Message #6 is received and validated (see below).

d. Upon receipt of Message #1 or alternatively if Message #2 was sent, upon the receipt of Message #3, **Message #4 Send Money Notification** is sent to the participants PayThat CashBox to confirm receipt of Message #1.

e. Upon receipt of Message #4, **Message #5 Send Money Notification** is sent to the payee (Participant 2 or S-2) via the method selected either email or text message. If an alias is used, the message is sent via the method selected by Participant 2 in the alias they established. Good funds are actually transferred with the PayThat Token(s) transferred in Message #5. All messages are encrypted, including Message #5 and the structure of the encrypted message has each individual XML tagged data element in the message separately encrypted, so that access to it can be variable based on role, authority, authentication status and need to know. No funds are transferred prior to this moment during a transaction. It is important to note that if S-2 cannot authenticate themselves to the IAF and/or to FI-2, they cannot open the .pay file and will not be able to deposit the funds into FI-2 or even view the contents of the .pay file or manipulate it in any way.

Payer’s provider (FI-1) will actually settle the transaction and move the good funds from FI-1 to FI-2, or in the use case where S-2 also banks with FI-1, FI-1 will transfer the good funds from S-1’s account at FI-1 to S-2’s account at FI-1, when it has received the authenticated, encrypted, untampered Message #1 and Message #3, and Message #6 has been received by FI-2 (or received by FI-1 in the alternative use case where FI-1 is also S-2’s Depository Institution) and FI-2 (or FI-1 in the alternative use case where FI-1 is also S-2’s Depository Institution) has informed FI-1 that Message #6 has been received. Individual transactions may be settled among Depository Institutions individually or in batch, on a net settlement basis, account to account, or via an existing legacy payment system such as FedACH or FedWire.
If some fraud, Regulation E related issues, AML or BSA issues has been detected or reported or a request from law enforcement is received to block an account to FI-1 or FI-2, either or both of FI-1 or FI-2 may reset the funds in S-1’s and/or S-2’s accounts or block funds in S-1’s or S-2’s accounts as necessary.

No PII is included in any of the payment messages one to eight. Each of these messages is fully encrypted in motion and at rest as described above.

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages should take under two seconds. For use cases where Sigma 5 or Sigma 6 reliability is required, more expensive and reliable networks with guaranteed uptime can be used to communicate among the parties involved in a transaction. Status of the transaction is available at all times to FI-1, FI-2, S-1 and S-2 once they transmit or receive the first message of the eight messages that they are involved in. Using modern commercial grade telco and internet networks the elapsed time from payment initiation to the point of completion including approval should take under two seconds. Settlement may occur within two seconds if FI-1 and FI-2 have an agreement to settle each transaction immediately, or at a different interval agreed among them, to a maximum of 30 minutes. Smaller Depository Institutions to participate in the PayThat Payment System must join as a member of one of the limited number of PayThat Clearing Banks, one of more of which may be member owned by smaller Depository Institutions. The only settlement transactions that smaller Depository Institutions that are not a PayThat Clearing Bank would be involved in would be End-User initiated transactions to move funds between legacy bank accounts at their Depository Institution and blocked funds accounts to fund a PayThat Payment System CashBox. Using the new real-time ACH system, these could be rapidly funded in either direction. The payment becomes final and irrevocable when the time related provisions of Regulation E have passed.

5. **Clearing**

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

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to clearing: E.4 (Payment format standards); S.7 (Security controls); S.9 (End-user data protection); F.2 (Fast clearing).
The PayThat Clearing Banks (FI-1 and FI-2) will utilize ISO20022 format payment messages embedded in all the messages between themselves. Messages number one through eight will also have ISO20022 formatted payment message data embedded as the payment kernel in each message. The PayThat Tokens are a cryptographic element and these are combined with a ISO20022 payment message and optionally XML enable e-invoicing data to create the payment instruction and payment information part of the encrypted messages. As noted above, each individual data element of the message is individually encrypted to enable variable access based on role, authority, confirmation of authenticated status and need to know.

Payer’s provider (FI-1) will actually settle the transaction and move the good funds from FI-1 to FI-2, or in the use case where S-2 also banks with FI-1, FI-1 will transfer the good funds from S-1’s account at FI-1 to S-2’s account at FI-1, when it has received the authenticated, encrypted, untampered Message #1 and Message #3, and Message #6 has been received by FI-2 (or received by FI-1 in the alternative use case where FI-1 is also S-2’s Depository Institution) and FI-2 (or FI-1 in the alternative use case where FI-1 is also S-2’s Depository Institution) has informed FI-1 that Message #6 has been received. Individual transactions may be settled among Depository Institutions individually or in batch, on a net settlement basis, account to account, or via an existing legacy payment system such as FedACH or FedWire.

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages should take under two seconds. For use cases where Sigma 5 or Sigma 6 reliability is required, more expensive and reliable networks with guaranteed uptime can be used to communicate among the parties involved in a transaction. Status of the transaction is available at all times to FI-1, FI-2, S-1 and S-2 once they transmit or receive the first message of the eight messages that they are involved in. Using modern commercial grade telco and internet networks the elapsed time from payment initiation to the point of completion including approval should take under two seconds. Settlement may occur within two seconds if FI-1 and FI-2 have an agreement to settle each transaction immediately, or at a different interval agreed among them, to a maximum of 30 minutes. Smaller Depository Institutions to participate in the PayThat Payment System must join as a member of one of the limited number of PayThat Clearing Banks, one or more of which may be member owned by smaller Depository Institutions. The only settlement transactions that smaller Depository Institutions that are not a PayThat Clearing Bank would be involved in would be End-User initiated transactions to move funds between legacy bank accounts at their Depository Institution and blocked funds accounts to fund a PayThat Payment System CashBox. Using the new real-time ACH system, these could be rapidly funded in either direction. However payment becomes legally final and irrevocable when the time related provisions of Regulation E have passed.
No PII is included in any of the payment messages one to eight. Each of these messages is fully encrypted in motion and at rest as described above. PII may be passed between FI-1 and FI-2 via a legacy payment system if required by the AML and BSA policies of either require it, but otherwise no PII is exchanged among any of the parties involved in a transaction (S-1, S-2, FI-1 and FI-2).

6. **Receipt**

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

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

To open the .pay file and access its contents including the money contained in it (and optionally contextual data such as e-invoicing information if such information is included also), S-2 must be an enrolled PayThat participant and authenticate themselves to the IAF (the Authentication Server) or log in to their Depository Institution’s participant’s existing online banking or mobile banking services. If S-2 is not an enrolled PayThat participant, they will receive a marketing message encouraging them to sign up and enroll in the PayThat Payment System to access the funds in the .pay file. This viral marketing technique is a form of super distribution. If S-2 is enrolled, authenticated, opens the CashBox and opts to deposit the money contained in the .pay file into their CashBox, Message #6 Deposit Money Notification is sent to FI-1, if S-2 is a customer of FI-1, or to FI-2, per the diagram.

Contextual data will be available to S-2, immediately upon receipt of Message #5, assuming S-2’s role, authority, need to know are delegated to it by either S-1 or the privacy template that S-1 has adopted for its PayThat payment message activity and the authentication status of S-2 is confirmed (see authentication, above). Data that is not needed to be known by other parties to a transaction will remain encrypted and unavailable to that party even if present in the .pay file. For example, account numbers need to be known by FI-1 and FI-2 but never by
S-1 or S-2, since their respective Depository Institutions know their customers via alternative means using the SSO or IAF process described above.

Based on the privacy template adopted by S-1 governing the data related to its transactions across the PayThat Payment System, based on authenticated status, role, authority and need to know, S-2 may opt to export any contextual data associated with a .pay file through an open API. This open API will have a help wizard that automates the process of pulling data into standard industry business and personal finance systems (e.g. accounts payable, accounts receivable, claims processing, payroll, treasury workstation, ERP systems, Consumer accounting software and tax reporting software).

Good funds are immediately available to S-2 to initiate a new payment to a third party upon opening the .pay file, assuming all the pre-conditions have been met (S-2’s role, authority, need to know are delegated to it by either S-1 or the privacy template that S-1 has adopted for its PayThat payment message activity, the CashBox is open and the authentication status of S-2 is confirmed). S-2 can then add the PayThat Token(s) included in the .pay file to the balance in S-2’s CashBox. Once present in the CashBox, they can be used to initiate additional good funds transactions.

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages, being all automated, should take under two seconds, 24/7/365. For use cases where Sigma 5 or Sigma 6 reliability is required, more expensive and reliable networks with guaranteed uptime can be used to communicate among the parties involved in a transaction.

Status of the transaction, including payment status, is visible and available at all times to FI-1 and FI-2 (as part of the PayThat Clearing Banks’ software), and to S-1 and S-2 (via their CashBox) once they transmit or receive the first message of the eight messages that they are involved in. Using modern commercial grade telco and internet networks the elapsed time from payment initiation to the point of completion including approval should take under two seconds, 24/7/365.

Settlement may occur within two seconds if FI-1 and FI-2 have an agreement to settle each transaction immediately, or at a different interval agreed among them, to a maximum of 30 minutes. Smaller Depository Institutions to participate in the PayThat Payment System must join as a member of one of the limited number of PayThat Clearing Banks, one of more of which may be member owned by smaller Depository Institutions. The only settlement transactions that smaller Depository Institutions that are not a PayThat Clearing Bank would be involved in would be End-User initiated transactions to move funds between legacy bank accounts at their Depository Institution and blocked funds accounts to fund a PayThat Payment System CashBox. Using the new real-time ACH system, these could be rapidly
funded in either direction. The payment becomes final and legally irrevocable when the time related provisions of Regulation E have passed.

If some fraud, Regulation E related issues, AML or BSA issues has been detected or reported or a request from law enforcement is received to block an account to FI-1 or FI-2, either or both of FI-1 or FI-2 may reset the funds in S-1’s and/or S-2’s accounts or block funds in S-1’s or S-2’s accounts as necessary.

All pending transactions are visible 24/7/365 in the Participant’s CashBox as pending authorized transactions. Specific details about pending status are also available including when their Depository Institution received and approved their payment request, when their Depository Institution account and CashBox has been debited, and when the payment was received by S-2 and cleared by FI-2 and FI-1. For S-1, this transaction detail would include when the payment was transmitted by them, when their Depository Institution received and approved the payment request, when their Depository Institution account and CashBox has been debited, and when the payment was received by S-2 and cleared by FI-2 and FI-1. For S-2, this transaction detail would include when the payment was transmitted to them, when their Depository Institution received and approved the payment request, when their Depository Institution account and CashBox has been credited, and when the payment was received by S-2 and cleared by FI-2 and FI-1.

No PII is included in any of the payment messages one to eight. Each of these eight messages is fully encrypted in motion and at rest as described above. PII may be passed between FI-1 and FI-2 via a legacy payment system to effect settlement of transactions if the AML and BSA policies of either require it, but otherwise no PII is exchanged among any of the parties involved in a transaction (S-1, S-2, FI-1 and FI-2).

Data quality and integrity is assured by means of the confirmations sent between the four parties to confirm receipt of each instruction and to validate that the contents of the encrypted files being used as receipts were not altered or tampered with following payment initiation.

Using the Foreign Exchange value added service of the PayThat Payment System, Dollar denominated PayThat Tokens can be exchanged for PayThat Tokens denominated in multiple currencies. Any currency or virtual currency can theoretically be supported by PayThat and a PayThat CashBox. The Foreign Exchange web service will utilize the domain names currency-exchange.com and currency-exchange.net.

For the following reasons the PayThat Payment System should see rapid adoption among the unbanked:

- over 70% of the unbanked in the United States use a smart phone;
- over 98% of the unbanked have an email address and use email communication;
the unbanked, like all United States residents, send many more text messages than email messages;
access to shared computers at public libraries enables the vast majority of all unbanked in the United States to have access to internet based services;
PayThat is email and text messaging based, intuitive and as easy to use as email and text messaging;
the cost of basic PayThat and PayThat transactions can profitably be set at a very low (versus legacy solutions) or zero cost;
overdraft fees can never be incurred.

In a consumer environment where guardianships (for elderly adults or minor children) or trustee relationships, or for married parties, two or more authorizations from two or more CashBoxes controlled by two or more Participants may be required to authorize a transaction and confirmation messages (including message #4, message #7 and message #8 may be copied and sent to one or more additional parties. In this way, dual control and approval based on hierarchies of authority can be enforced. A fully competent adult can be a second approver for a less than fully competent individual, while still providing the less than fully competent individual a higher degree of financial autonomy with less risk. If required or desired, dual control can be established using two or more fully competent adults, the second of whom has “approval only” or “read only” authority. This method can reduce or even eliminate financial abuse of minor children, minimally competent adults and elder financial abuse.

PayThat messages use either SMTP (email) or SMS (text messaging) message standards to enable device and system interoperability.

All fees (authorized at initiation of a payment) will be recorded in the PayThat Payment System Cleared Transactions database, and also in the cleared transactions database associated with the participant’s CashBox.

As noted above the PayThat Payment System supports a large number of use cases comprehensively.

The individual receipts for each completed transaction stored in a Participant’s CashBox have a button a Participant may manually trigger that automatically reports a transaction to FI-1 as fraudulent, erroneous or unauthorized. Similarly, upon receipt of a .pay file, S-2 may flag a transaction by manually triggering a button that automatically reports a transaction to FI-1 and/or FI-2 as applicable, as fraudulent, erroneous or unauthorized. Such requests will be handled under Depository Institutions’ existing standard error resolution process under Regulation E and in the timeframes currently applicable.
7. Settlement

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

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

The PayThat Payment System holds stored value in the form of good funds within blocked bank deposits for funds deposited into the payment network and supports push payments only; legacy business models utilizing debit pull today can be fully supported in a good funds environment with revocable prior authorization automation by participants that then lead to push payments.

The blocked bank accounts can only be credited or debited by the Depository Institution that holds the bank account. When End-Users direct FI-1 to perform a push payment to S-2’s account (either at FI-1 or FI-2), FI-1 performs the push payment using good funds to that new account, and new Depository Institution if S-2 is a customer of FI-2 and not FI-1.

Because the PayThat Payment System only transacts in good funds using central bank money there is only minor residual settlement risk, as even in the event of the collapse of FI-1, the bank deposit accounts that each CashBox is linked to, is FDIC-insured up to $250,000 per insured party (with some types of accounts the effective amount insured can be greater, for example, a joint account with two owners that is insured to $500,000, $250,000 each). The only settlement risk would therefore be that FI-1 fails prior to effecting settlement, the institution is liquidated or sold with the buyer not honoring deposits above the insurance limit and the account balance is above the insurance limit for each insured party.

Since banks that participate in the PayThat Payment System that are Clearing Banks would typically settle immediately (two seconds or less 24/7/365) or on a net basis periodically throughout the day (for example if the net accumulated amount owed is over $200,000 or within 30 minutes, whichever occurs first), the typical settlement would always be set at 30 minutes or less. Smaller Depository Institutions would typically be correspondents of these larger PayThat Clearing Banks (e.g. FI-1 and FI-2) and provide cash compensating balances or establish lines of credit to support settlement in these time frames.
Actual settlement may be immediate (two seconds or less) or batch, as established by prior agreement of the two Depository Institutions. Per the prior agreement of the Depository Institutions, this settlement may either be via ACH and/or FedWire exchanged between the actual Depository Institutions themselves or on a net settlement basis, account to account, where on Depository Institution holds a deposit at the other which is debited or credited as transactions settle. Actual settlement occurs only after Message #6 is received and validated (see above).

Regulated Non-Bank Account Providers are not allowed to be PayThat Clearing Banks and only Depository Institutions are allowed to provide PayThat deposit accounts to End-Users. There will be a limited number of PayThat Clearing Bank licenses. One or more Depository Institutions may have shared ownership of a PayThat Clearing Bank license, similar to existing bankers’ banks.

Since the PayThat Payment System operates 24/7/365 and settlement via legacy ACH and Wire systems are not available on holidays and non-business days, the PayThat Payment System rules will require good funds to be held in central bank money escrow accounts in an amount designed by analysis and historical and projected flow of funds to ensure that sufficient funds are available to cover the net settlement risk among PayThat Clearing Banks and smaller Depository Institutions that are correspondents of PayThat Clearing Banks, to cover their obligations under Sigma 4, Sigma 5 or Sigma 6 probability, as determined by the PayThat Payment System rules. PayThat Clearing Banks will be required to operate and continue settlement at extended hours to enable transactions in all time zones in the United States to have normal business hours in their own time zone.

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

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

S-1 can initiate a payment to S-2 with only the knowledge of S-2’s email address, cell phone number or alias (aliases are listed in the CIF Database and optionally broadcast on a variable basis to authenticated and enrolled End-Users based on the participants privacy templates where participants can mandate who has access to their data by role and authority). S-1
would never have access to any other data related to S-2 unless S-2 shared that data outside of band outside the PayThat Payment System or it was data originated by S-1 related to a transaction initiated by S-1 that is subsequently received by S-2. S-1 and S-2 do not and cannot learn account number or other PII data of the other at any point throughout the end-to-end payment process.

All transaction messages that flow across the PayThat Payment System Clearing Banks (e.g. FI-1 and FI-2) are copied to one or more of the four PayThat databases:

- The Authentication Server database records all authentication sessions of the IAF.
- The Pending Transactions database records every of the following payment messages: #1, #2, #3, #4, #6, #7.
- The CIF Database records all initial enrollment sessions of the IAF and all modifications or incremental enrollment sessions after the initial enrollment session.
- The Cleared Transactions Database records every of the following payment messages: #1, #2, #3, #4, #6, #7 along with the confirmation from FI-1 and FI-2, if S-2 is not FI-1’s customer, that settlement has or has not yet occurred and when and via what transaction across which legacy payment system.

Each of the records located in these four databases are encrypted using cryptographic standards so that each data element is separately encrypted such that data elements are accessible solely and variably based on role, authority, authentication status and need to know. Data elements are persistently secured and encrypted, so that data can travel freely across the cloud, databases or insecure systems/networks as an encrypted, secure data element and still be access controlled solely based on role and authority.

All data in the four PayThat Payment System databases and all communications between the PayThat Clearing Banks and the four databases are encrypted at motion and at rest using ANSI X-9 and ISO Standard cryptographic methods.

Research of the pending transactions and cleared transactions by law enforcement and the Federal Reserve’s economic research unit can be facilitated based on role, authority and a need to know. For example, law enforcement may need to know the identity of the End-Users involved in a transaction but not some data elements about some transactions, such as health-care related data controlled by HIPAA related to heart surgery. Those data elements could not be unlocked for research purposes without a judge’s court order digitally signed granting them authority based on need to know. The Federal Reserve’s economic research unit could gain access to real-time data on transaction sizes and goods being sold across the economy but not need to know the identity of the End-users involved in the transaction. Those data elements would remain encrypted and not be accessible to the researchers based on their lack of a need to know.
If some fraud, Regulation E related issues, AML or BSA issues has been detected or reported or a request from law enforcement is received to block an account to FI-1 or FI-2, either or both of FI-1 or FI-2 may research the transaction and all electronic sessions related to it by querying the four databases. If necessary a PayThat Clearing Bank may reset the funds in an End User’s accounts or block funds in an End User’s accounts as necessary.

Pending transactions and the individual receipts for each completed transaction stored in a Participant’s CashBox have a button a Participant may manually trigger that automatically reports a transaction to FI-1 as fraudulent, erroneous or unauthorized. Similarly, upon receipt of a .pay file, S-2 may flag a transaction by manually triggering a button that automatically reports a transaction to FI-1 and/or FI-2 as applicable, as fraudulent, erroneous or unauthorized. Such
requests will be handled under Depository Institutions’ existing standard error resolution process under Regulation E and in the timeframes currently applicable. The payment becomes final and legally irrevocable when the time related provisions of Regulation E have passed.

Liability and financial responsibility, liability limits for transactions and timeframes for addressing all issues are also apportioned among the End-Users and PayThat Clearing Banks based on the provisions of Regulation E. For End-Users located in those states, PayThat Payment System will comply with any state law that imposes protections that are greater than that provided under Regulation E (see Section 919 of the Act).

PayThat Payment System does not involve credit transactions except when a linked account that funds a CashBox is a credit type bank account, so Regulation Z is generally not applicable, however to the extent that Regulation Z is applicable the PayThat Payment System will comply with and follow the provisions of Regulation Z for credit related transactions in apportioning the Liability and financial responsibility, liability limits for transactions and timeframes for addressing all issues among the End-Users and PayThat Clearing Banks.

Any additional fees for additional optional services of any type will be fully disclosed and shall require the consent of the Participant prior to completion of the Authorization process and release of any good funds by the CashBox. Overdrafts are never allowed and overdraft fees are never incurred in the PayThat Payment System.

PayThat messages and messages to the CashBox of a Participant regarding error and complaint resolution use either SMTP (email) or SMS (text messaging) message standards to enable device and system interoperability.

All data in the four PayThat Payment System Databases shall be stored for seven years to facilitate research in line with the needs of industry to research tax related issues related to payments. After seven years, the encrypted data elements cannot be accessed regardless of role, authority or a need to know. Optionally, some data elements may have a shorter shelf life if the PayThat Payment System rules require it in compliance with applicable laws and regulations.

All nodes in the PayThat Payment System will be protected by state of the art cyber security protection, monitoring and malicious pattern detection systems that perform and facilitate data breach prevention and detection. For example, the Promia Raven, which protects the data centers of the U.S. Navy’s Network Operating Centers, would be a good candidate vendor solution, however the actual system would be selected following an RFP. The IAF will manage the cyber security protection, monitoring, malicious pattern detection and data breach prevention and detection systems for the four databases, as well as data breach reporting for the PayThat Payment System, the IAF and the PayThat Clearing Banks.
The IAF will be responsible for facilitating timely and frequent sharing of information among all Providers, operators and regulators to help them manage, monitor, and mitigate Fraud and evolving threats in accordance with applicable law. The PayThat Payment System rules, led by the IAF, shall require the sharing of information to facilitate managing and monitoring Fraud including:

- detection of patterns at the individual or aggregate level suggestive of risk;
- known instances of Fraud;
- known vulnerabilities;
- the significance of the information; and
- effective mitigation techniques.

Information shared for anti-fraud activities shall be used only for fraud management purposes and this will be enforced by the encryption of the data elements shared. All data shared shall remain fully encrypted at rest and in motion, including PII, and PII shall be excluded from information sharing when possible. If shared, data shall only be accessible based on role, authority, authentication status and need to know.

Since Level 3 and Level 4 authentication will utilize as a part of the process a web service that generates an email message with a .post.us top level domain from the Authentication Server to the IAF confirming authentication of the End-User, any identity based fraud will be investigated by the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal Service. Also, through an existing treaty through the Universal Postal Union (UPU), any attempted or actual identity fraud in any of 190 member countries of the UPU, each of which have their own Postal Inspection Service law enforcement agency, is capable of being investigated by that country’s Postal Inspection Service law enforcement agency.

The four databases and each PayThat Clearing Bank will be physically housed in enterprise network server data centers compliant with FFIEC standards for vendors for Depository Institutions. The data centers will incorporate (the following list is intended only to highlight at a high level some of the many FFIEC standards) policies, procedures and rules regarding:

- Physical security including physical access security
- Network monitoring and incident response
- Business disaster recovery and business resiliency & target availability plans and policies
- Enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process
- Internal and external audits
- An annual Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, SSAE 16
- Periodic contingency testing and mock disaster scenario drills across the PayThat Payment System.
- Change management including those caused by technology and regulation changes
In Pursuit of a Better Payment System
Faster Payments Task Force

- Internal or external fraud or errors
- Periodic review and update
- Sigma 6 uptime, by ensuring all mission critical systems have geographically separated immediate fail-over redundancy, including POPs, servers and web services.

A full list of FFIEC standards can be reviewed by accessing the examiner guides of the FFIEC bank regulatory agencies. As a vendor to 373 other financial institutions, University Bank clearly has excellent FFIEC IT compliance.

The PayThat Payment System rules that all Providers must agree and adhere to via a participation agreement, will ensure that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules, including those applicable to End-Users and that the PayThat Payment System can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures.

Comments on Legal Framework and Governance of the PayThat Payment System

The PayThat Payment System is designed to operate within existing laws without any changes being required.

Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The following legal principles, rules and policies will be incorporated into these Governance Documents:

1. All laws, regulations, regulatory interpretations or rulings, court decisions (collectively “Laws”) and/or PayThat Payment System Rules that will apply to the Payment System, End Users, Providers, Payers and Payees, and payments through the PayThat Payment System.
2. Specificity as to how Entities and the payments themselves that transact through the PayThat Payment System will be legally bound to the PayThat Payment System Rules.
3. A statement as to the adherence of the PayThat Payment System to all applicable legal requirements and responsibilities and specificity as to the allocation of responsibilities and liabilities for the compliance with all applicable federal, state, local and international Laws.
4. Codification into specific written rules of the PayThat Payment System Rules regarding enrollment, authentication, Messages #1 through #8, the IAF, the operations and records stored in the four databases, the PayThat Clearing Banks, Value Added Services, the error resolution, receipts and records process, the authority of the PayThat Payment System to examine and audit Entities and sanction and if necessary expel them from the PayThat Payment System & etc., as described in this document.
5. The governance model, voting and amendment process by class of Entity and the process for obtaining input from PayThat Payment System stakeholders including:
   - Governance arrangements (e.g., policies and structure) that shall ensure efficient decision making and rule making, including establishing clear lines of responsibility for all decision makers or decision-making bodies.
   - A requirement for the public disclosure of the governance arrangements.
   - The governance arrangements should provide a process to handle appeals related to specific decisions or their implementation.
   - The governance arrangements should provide for independent validation of compliance with the Rules, compliance with applicable law, and achievement of both PayThat’s objectives and public policy objectives.
   - The governance arrangements should include consideration of the public interest when making decisions and rules.
   - The governance arrangements should provide for input and influence by all stakeholders, through one or more governance or advisory bodies.
   - PayThat should have governance and advisory bodies that fairly represent stakeholders’ interests and risks.
   - PayThat’s governance approach should enable specific stakeholders or stakeholder groups to proportionately influence outcomes.
   - PayThat’s governance approach should address and manage actual, perceived, or potential conflicts of interest.
   - PayThat’s governance approach should incorporate Public Policy Objectives that promote safe, efficient, and accessible payments with appropriate protections for End Users.

6. The allocation of losses due to the failure by the IAF, a Depository Institution or a PayThat Clearing Bank to properly vet End-Users during enrollment and authorization or due to a data breach.

7. Rules under which PayThat Clearing Banks or the PayThat Payment System itself may optionally establish for End Users and/or Providers additional Consumer protections for payments, which may exceed those protections that are otherwise required under applicable law.

Part A, Section 2: Use Case Description

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

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported. Transaction data interchange is optionally fully supported to automate STP and ERP integration. Example payments supported: (ad hoc low value) Just-in-time supplier payments, supply chain e-invoicing, Cross Border Single Window Trade Facilitation payments and data exchange, Health Information Exchange related payments</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
</tbody>
</table>

In the B2B use case, a payment is sent by a business or government End-User to a business or government End-User. Payments may be sent with no contextual data however typically some contextual data is sent and the default option is for the CashBox to request all the contextual data required to transmit a STP820 message which is an ISO20022 compliant message containing only the extra limited set of data required for over 95% of all B2B business transactions to settle with straight through processing (STP) and no error resolution or reconciliation process being then required following receipt. The contextual data may optionally be more data rich X12, ISO20022 data or UN CEFACT XML data. A button in the CashBox allows S-1 to upload data sourced from any file accessible from S-1’s device (e.g. ERP system data). This process can also be automated so that the CashBox is directly integrated into the ERP system process provided that the authentication status of S-1 (and optionally S-1b if dual control, as discussed in greater detail below, is required) is validated by S-1’s Depository Institution or the IAF. Whether or not data is attached to the Messages, the message flow is identical to the processes described in the
sections above. The flow of messages is identical. The order of actions (as described in Part A, Section 1, Solution Description, above) is:

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

Based on the privacy template adopted by S-1 governing the data related to its transactions across the PayThat Payment System, based on authenticated status, role, authority and need to know, S-2 may opt to export any contextual data associated with a .pay file through an open API. This open API will have a help wizard that automates the process of pulling data into standard industry business and personal finance systems (e.g. accounts payable, accounts receivable, claims processing, payroll, treasury workstation, ERP systems, Consumer accounting software and tax reporting software). At a minimum, even if a specific API isn’t available for a system, the open API data can as a default be exported using comma delimited excel files, since excel is the most common software used to support business data interchange.

The open API for exporting data and the ability to import contextual data also through an open API enables vendors of any type to provide an ecosystem of value added services. Any of these value added services would be required under the PayThat Payment System rules to fully disclose to any End-User opting to use these services any fees for these additional optional services and that these services are optional, prior to incurring any fees.
Cross-border functionality is provided by a Global Payment Gateway connected to global legacy payment systems.

The Global Payment Gateway:

The Global Payment Gateway (GPG) is a web service built by Depository Institutions that communicates through and leverages legacy payment networks in each country around the world to enable cross-border payment functionality in real-time leveraging RTGS payment systems around the world. The concept was first piloted in the Universal Value eXchange (UVX) pilot of the Financial Services Technology Consortium (FSTC). Several major banks have since built GPGs including Wells Fargo and Chase Bank. The PayThat Payment System would either
In Pursuit of a Better Payment System

Faster Payments Task Force

utilize one or more of the existing GPGs selected by RFP, or build a new one in partnership with a large bank selected via RFP. In the diagrams the circles “Legacy Payments Network” are assumed to include both domestic and international payment networks and the GPG functionality as these are typically existing integrated solutions inside the payments line of business at most large banks. The author was the Deputy Project Manager of the FSTC’s UVX project and University Bank was one of the two banks that piloted and proved the technical feasibility of the UVX GPG concept.

A GPG is constructed by having a bank be a member of the local ACH or Wire (RTGS) payment systems or possess a correspondent bank deposit account at a bank that is a member of each payment system in each country in which payments are to be sent or received from. This allows the bank to bypass SWIFT and using the real-time payment systems already built that connect to each bank in each country, to send or receive real-time payments globally. GPG services are always an extra valued added service with an additional fee. When exchanging currency from one type to another foreign exchange fees are also earned.

When a payment includes contextual data, the GPG backbone allows the contextual data to pass in a secure environment between a corporate ERP or accounting system, one or more Depository Institution(s) and the existing payment systems resident in each country around the world. Transactions using GPG:

- Are assured as to finality of payment
- Very fast
- Enable payment finality with real-time settlement
- Are based on the UVX protocols
- Minimize human intervention and error
- Allow real-time management of accounts receivable or accounts payable exceptions by either party to a transaction
- Are low cost
- Are affordable for all suppliers and customers

The GPG is a bank-centric network. The IAF or the End-User corporation’s Depository Institution will provide the GPG with identity assurance and authentication authorization when accessing the GPG. Payments are processed to and from the preexisting Depository Institution accounts now used by the Corporation’s cash management department. Payment initiation can be achieved through a web-interface, existing corporate cash management software, email or SMS based text messaging. The payment cycle can be completed and settled within seconds or delayed for release at a time and date specified in advance, assuring the corporation that payment is made and is final. The ultimate method of payment would cut across many different platforms, and could include credit card, debit card, ACH, FedWire, SWIFT, telco and wireless payment systems, international country specific legacy payment networks and all data associated with the transaction can incorporate information rights management (i.e. encryption of all data elements
Components of the GPG:

a. A series of transaction gateways that can convert payment kernels (i.e. payment instructions) from one payment system format to another.

b. A universal data dictionary that uses industry standards for defining the structure of payment system transactions (e.g., XML, ebXML) and the mapping of one payment vocabulary to another.

c. The functionality should allow the originator to control the day the item settles (good funds). [Corporations big and small as well as individuals all hate losing control of payment finality] Therefore there should be a pending transactions database between the incoming and outgoing payment messages. This database would have status of all transfers available in real-time. The database could optionally be the PayThat Payment System Pending Transactions database.

d. The Corporation would transmit just one type of payment instruction to the GPG and receive back from the GPG payment advices in just one standard format. The payment kernels of these messages are ISO20022 compliant.

The GPG would be built using a sequential development program (in 90 day units) to gain traction for the UVX project with a view towards a bigger game plan/vision that we were building to, including:

a. Add all the other international payment flavors in little 30-90 days increments one by one (or if available in groups).

b. Build a robust and fault tolerant TCP/IP based system.

c. Move financial EDI/ERP/accounting data with transaction data.

d. Create a one-stop merchant or customer sign-up web interface (commercialization phase), which optionally could be the IAF.

Adoption Plan

First, identify a core customer that needs global payment options in local currency accounts.

Phase 1:

Build a U.S./Canada switch. This is easy to test and build out.

Phase 2:

Establish a European roll-out strategy. Roll out country by country based on the priority of top pilot businesses. Each country in Europe can be accessed from the ACH and...
RTGS payment system of one single European country at no extra cost due to the EU Government’s SEPA mandate.

Phase 3:

Establish a U.S./Mexico switch.

Phase 4:

Establish a roll-out strategy for other regions based on the priority of top pilot businesses.

The Fed’s Global ACH could alternatively be used as a GPG to fund foreign currency denominated bank deposits that are blocked and associated PayThat Tokens deposited to a CashBox denominated in a foreign currency, provided that the Fed’s Global ACH transactions can be sent in multiple currencies without first requiring conversion into U.S. Dollars. If S-1 desires a transaction to be initiated in foreign currency, S-1 must authenticate to the CashBox and use the foreign exchange button in the CashBox to exchange PayThat Tokens denominated in U.S. Dollars for PayThat Tokens denominated in the desired currency. The required amount of the foreign currency may be specified during this process or a fixed amount of U.S. Dollars may be exchanged into a desired foreign currency. Prior to authorizing the exchange, all fees, rates and terms charged by FI-1 for providing the service are disclosed to S-1, and S-1 confirms affirmatively that it wishes to incur those fees and continue with the proposed transaction. Then the CashBox displays the balance on deposit in all available currencies and a participant may select the currency desired to initiate a payment. Upon receipt S-2 may also perform the same foreign exchange service with FI-2, or FI-1 if it is a customer or FI-1.

Dual Control with Business or Government Payments

Optionally, the business or government may have dual control to prevent fraud and reduce errors and as a result, two participants of those end users would be required to first authenticate and authorize the payment before Message #1 is able to be sent. A message is sent to Participant #2 from Participant #1’s CashBox when a payment is initiated to obtain approval from Participant #2. The order of actions (with specifics as described in Part A, Section 1, Solution Description, above) is:

1a. Authentication, Participant #1
2a. Initiation, Participant #1
3a. Payer Authorization, Participant #1
1b. Authentication, Participant #2
3b. Payer Authorization, Participant #2
4. Approval by the Payer’s Provider

5. Clearing

6. Receipt

7. Settlement

8. Reconciliation

In this optional use case, Message #0a and Message #0b are sent prior to Message #1 being generated. Based on the privacy template adopted by the End-User associated with S-1, the CashBox of S-1 automatically sends Message #0a to the participant designated to be the dual control approver in the privacy template, Participant 1b (S-1b). S-1b then approves the transaction and the CashBox of S-1b automatically generates Message #0b. Upon receipt by the CashBox of S-1, Message #1 is automatically generated, following the same flow of messages from that point forward.
PayThat Solution Message Flow & Elements

**Depository Institution 1 (FI-1)**

- **MSG # 1**: Confirm FI-2’s receipt of FWD: BCC: S-1 Send Money Notification MSG # 3
- **MSG # 2**: BCC: S-1 Send Money Notification MSG # 4
- **MSG # 3**: Confirm Receipt of FWD: BCC: S-1 Send Money Notification MSG # 2

**Participant 1 (S-1)**

- **MSG # 5**: S-1 Send Money Notification MSG # 6
- **MSG # 0a**: S-1 Send Dual Control Request MSG # 0a
- **MSG # 0b**: S-1 Send Dual Control Request MSG # 0b

**Depository Institution 2 (FI-2)**

- **MSG # 4**: FWD: BCC: S-1 Send Money Notification MSG # 4
- **MSG # 7**: Confirm S-2 Deposit Money Notification MSG # 8
- **MSG # 8**: S-2 Deposit Money Notification MSG # 8

**Participant 2 (S-2)**

- **MSG # 6**: S-2 Deposit Money Notification MSG # 6
## Supported use case coverage summary

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td><em>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported including ad hoc low value and ad hoc high value. Example payments supported: Wages for temporary workers or time sensitive corrected payroll (ad hoc low value), Medical insurance claims, legal settlements, FEMA transfers (ad hoc high value)</em></td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
</tbody>
</table>

In the B2P use case, a payment is sent by a business or government End-User to a person. Only a payment is sent and no contextual data. It is identical to the processes described in the sections above. The flow of messages is identical. The order of actions (as described in Part A, Section 1, Solution Description, above) is:

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

If S-1 desires a transaction to be initiated in foreign currency, S-1 must authenticate to the CashBox and use the foreign exchange button in the CashBox to exchange PayThat Tokens denominated in U.S. Dollars for PayThat Tokens denominated in the desired currency. The required amount of the foreign currency may be specified during this process or a fixed amount
of U.S. Dollars may be exchanged into a desired foreign currency. Prior to authorizing the exchange, all fees, rates and terms charged by FI-1 for providing the service are disclosed to S-1, and S-1 confirms affirmatively that it wishes to incur those fees and continue with the proposed transaction. Then the CashBox displays the balance on deposit in all available currencies and a participant may select the currency desired to initiate a payment. Upon receipt S-2 may also perform the same foreign exchange service with FI-2, or FI-1 if it is a customer or FI-1.

**Message Flow B2P (No Dual Control, No Contextual Data)**

---

**PayThat Solution Message Flow & Elements**

---

**Message Flow B2P (With Dual Control, No Contextual Data)**
Optionally, the business or government may have dual control to prevent fraud and reduce errors and as a result, two participants of an End-User would be required to first authenticate and authorize the payment before Message #1 is able to be sent. An encrypted .pay message is sent to Participant #2 from Participant #1’s CashBox when a payment is initiated to obtain approval from Participant #2. The order of actions (with specific details as described in Part A, Section 1, Solution Description, above) is

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

In this optional use case, Message #0a and Message #0b are sent prior to Message #1 being generated. Based on the privacy template adopted by the End-User associated with S-1, the CashBox of S-1 automatically sends Message #0a to the participant designated to be the dual control approver in the privacy template, Participant 1b (S-1b). S-1b then approves the transaction and the CashBox of S-1b automatically generates Message #0b. Upon receipt by the CashBox of S-1, Message #1 is automatically generated, following the same flow of messages from that point forward.
PayThat Solution Message Flow & Elements

- **Depository Institution 1 (FI-1)**
- **Depository Institution 2 (FI-2)**
- **Participant 1 (S-1)**
- **Participant 2 (S-2)**
- **Participant 1b (S-1b)**

- **MSG # 1**: Confirm FI-2's receipt of FWD: BCC: S-1 Send Money Notification MSG # 3
- **MSG # 2**: FWD: BCC: S-1 Send Money Notification MSG # 4
- **MSG # 3**: BCC: S-1 Send Money Notification MSG # 5
- **MSG # 4**: Confirm S-2 Deposit Money Notification MSG # 7
- **MSG # 5**: S-1 Send Money Notification MSG # 8
- **MSG # 6**: FWD: Confirm S-2 Deposit Money Notification MSG # 8
- **MSG # 7**: S-2 Deposit Money Notification MSG # 8
- **MSG # 8**: S-1 Send Dual Control Request MSG # 4a
- **MSG # 9**: S-1 Send Dual Control Request MSG # 4b

Legacy Payments Network
In Pursuit of a Better Payment System

Faster Payments Task Force

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>The solution assists business, consumers and governments to make payments. All payment types and participant types are supported. Example payments supported: emergency bill payment, time-sensitive corrected bill payment, media and web services related micropayments, First Class Email related micropayments, Health Information Exchange related payments</td>
<td>Cross-border functionality is provided by a global payment gateway connected to global legacy payment systems.</td>
</tr>
</tbody>
</table>

In the P2B use case, a payment is sent by a person End-User to a business or government End-User. Usually only a payment is sent and no contextual data. It is identical to the processes described in the sections above. The flow of messages is identical. The order of actions (as described in Part A, Section 1, Solution Description, above) is:

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

If S-1 desires a transaction to be initiated in foreign currency, S-1 must authenticate to the CashBox and use the foreign exchange button in the CashBox to exchange PayThat Tokens denominated in U.S. Dollars for PayThat Tokens denominated in the desired currency. The required amount of the foreign currency may be specified during this process or a fixed amount of U.S. Dollars may be exchanged into a desired foreign currency. Prior to authorizing the exchange, all fees, rates and terms charged by FI-1 for providing the service are disclosed to S-1, and S-1 confirms affirmatively that it wishes to incur those fees and continue with the proposed transaction. Then the CashBox displays the balance on deposit in all available currencies and a
participant may select the currency desired to initiate a payment. Upon receipt S-2 may also perform the same foreign exchange service with FI-2, or FI-1 if it is a customer or FI-1.

**PayThat Solution Message Flow & Elements**

In the optional use case that the person End-User desires to send an invoice number, transaction reference number or the contextual data required to build and then transmit a STP820 message, the CashBox options menu can be accessed by S-1 to assist step by step with that process. The STP820 is an ISO20022 compliant message containing only the extra limited set of data required for over 95% of all P2B business transactions to settle with straight through processing (STP) and no error resolution or reconciliation process being then required following receipt. The message flow in this optional use case is identical to the processes described in the sections.
above. The flow of messages is identical. The order of actions (with specific details as described in Part A, Section 1, Solution Description, above) is:

1. Authentication
2. Initiation
2a. Creation of the STP820 or adding the invoice number to the payment during initiation
3. Payer Authorization
4. Approval by the Payer’s Provider
5. Clearing
6. Receipt
7. Settlement
8. Reconciliation

In this case the .pay file contains not just the payment kernel but the contextual data related to that transaction.

Contextual data may be added into the .pay file data fields by S-2 during the transaction message flow. For example, information about the amount of loyalty or rewards points earned and current points owned could be added into Message #8 as additional contextual data. All such data would be encrypted using the same methods as described above.
PayThat Solution Message Flow & Elements

Legacy Payments Network

Depository Institution 1 (FI-1)

Depository Institution 2 (FI-2)

Participant 1 (S-1)

Participant 2 (S-2)

B2B EXCHANGE (Optional)

www.PayThat.com

$ .PAY

© 2016 Federal Reserve Banks & University Bank. Materials are not to be used without consent.
In the P2P use case, a payment is sent by a person End-User to another person End-User. Only a payment is sent and no contextual data. It is identical to the processes described in the sections above. The flow of messages is identical. The order of actions (as described in Part A, Section 1, Solution Description, above) is:

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

If S-1 desires a transaction to be initiated in foreign currency, S-1 must authenticate to the CashBox and use the foreign exchange button in the CashBox to exchange PayThat Tokens denominated in U.S. Dollars for PayThat Tokens denominated in the desired currency. The required amount of the foreign currency may be specified during this process or a fixed amount of U.S. Dollars may be exchanged into a desired foreign currency. Prior to authorizing the exchange, all fees, rates and terms charged by FI-1 for providing the service are disclosed to S-1, and S-1 confirms affirmatively that it wishes to incur those fees and continue with the proposed transaction. Then the CashBox displays the balance on deposit in all available currencies and a participant may select the currency desired to initiate a payment. Upon receipt S-2 may also perform the same foreign exchange service with FI-2, or FI-1 if it is a customer or FI-1.
Part A, Section 3: Use Case by Effectiveness Criteria

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

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

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

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

1. Implementation Timeline

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

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

Because the PayThat software has been fully mapped and modeled in Unified Modeling Language (UML), including all primary and optional use cases and services, the software itself could be written in six months with alpha and beta testing completed within three months after that. The same CashBox software will be used by all Parties in the PayThat Payment System. The use cases and optional use cases modeled and mapped in UML are available under a Mutual Non-Disclosure Agreement (MNDA) for review.

Building the PayThat Clearing Bank software should take six months and can be done in parallel from day one, since it has relatively limited functionality and is designed and architected to be a completely autonomous unit that has only limited integration and points of interoperability with the associated Depository Institutions. Each PayThat Clearing Bank can utilize the same software suite. Eight to twelve PayThat Clearing Bank licenses are anticipated to be sold, including eight U.S. licenses and four licenses to overseas banks. PayThat Clearing Banks must process and react to the PayThat messages and interact with the four PayThat databases and the eight to twelve other PayThat Clearing Banks, and be able to send payments to and receive payments from the main domestic legacy payment system and/or a Global Payment Gateway (GPG) at a Depository Institution.
Customer complaints and fraud reports can be handled by existing bank operations and existing channels for handling Regulation E issues. Instances of identity fraud will be referred to the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal Service.

The Identity Assurance Federation manages the four databases and the main task is to build those databases pursuant to ISO encryption standards and the methods taught in the patents of Jove Corporation and TecSec, so that each data element is individually accessible or not accessible, based on authenticated status, role, authority and need to know. The databases should be able to be built and tested in three to six months, again in parallel from day one. The IAF will be used by all Parties in the PayThat Payment System.

Details on the Global Payment Gateway (GPG) and its implementation timeline are available above. If an existing GPG from one or more of the major global banks is used, this has the merit of being a quick one to three month implementation timeline. If the GPG is built in partnership with a major global bank, it will take six to twelve months to do so, and again can be done in parallel from day one. If an existing GPG is used, global payment system operability and multi-currency ubiquity can be achieved immediately at launch of PayThat. If the GPG is built, this system operability and ubiquity will increase rapid over the first 18 months following launch until it is ubiquitous.

The total cost of the programming for the above tasks is probably under $5 million and certainly under $10 million. Considering the fact that the value of the PayThat business is $1 billion to $10 billion under conservative estimates, and that FinTech venture capital firms are routinely funding dozens of deals this size per quarter, the funding should be readily available from the FinTech venture capital community, however, the Depository Institutions should and may fund the cost themselves without any need for outside venture capital. Additional costs will be incurred for the four specific use cases as is discussed in that section, below.

The chosen initial use cases are designed to achieve 40% market share of the market segment within 18 months following launch. This assures that PayThat will always have the number one market share in its chosen segments and will never be relegated to the number two market share position.

Having been involved in eight financial services start-ups in my career to date, with only one partial failure that was ultimately made profitable and turned-around, the author of this document can state with certainty that the cost and timelines are reasonable. Having said that, in my experience and the experience of entrepreneurs, tasks are typically delayed through unforeseen difficulties and a good rule of thumb is to double the time required and the funds required to go to market. This is why the $10 million number has been put forward. The outer timeline is 18 months.
Because University Bank would not be allowed by its primary banking regulator to launch the PayThat service on its own due to the AML/BSA risk they perceive in community banks operating innovative payment systems, at a minimum a large regional bank or ideally one or more of the large global Depository Institutions already involved in the Faster Payments Task Force or Secure Payments Task Force is required to partner to launch PayThat. University Bank will not launch PayThat if one or more of these much larger banks is not willing to take the lead as the initial PayThat Clearing Bank. University Bank did obtain the commitment of one of the four biggest U.S. global banks to roll out PayThat to their customer base if University Bank would pay for building the system, so we already have had one experience where this dependency has been overcome. Unfortunately, the global IT vendor who had committed to fund the build out at that time in exchange for a share of the profits of the PayThat Payment System, changed their minds and withdrew from the project. Since there is a critical mass of interested institutions already at the Faster Payments Task Force and Secure Payments Task Force, we firmly believe that this barrier to implementation can be overcome.

We have also carefully chosen initial use cases for adoption where there is no quality incumbent solution that needs to be displaced. In fact, there is a strong desire for any kind of workable solution in the chosen initial use cases (see Value Proposition and Competition, below).

2. Value Proposition and Competition

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

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

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

We have also carefully chosen initial use cases for adoption where there is no quality incumbent solution that needs to be displaced. In fact, there is a strong desire for any kind of workable solution in the chosen initial four use cases.
Targeted Use Case #1 Healthcare Payments

Problem Statement

The healthcare sector is the largest single industry in the U.S., contributing 17.6% of the nation’s GDP, however it has the lowest adoption of electronic payments with 95% of healthcare related payments ending up at some point in the payment process as a paper check. Also, administrative overhead is high at 30% of overall costs because healthcare claims data and healthcare clinical data are siloed in separate business processes and reconciliation between the two silos is time consuming and expensive. Healthcare providers, because they typically only rely on user name and password to access HIPAA controlled PII and have rarely deployed encryption to protect their data, have experienced rapidly rising security breaches that have compromised the health data privacy of over 100 million citizens just in the last year. As a result, they are open to outsourcing their identity management web services to the banking industry, which they recognize as having much stronger cyber security.

Elevator Pitch

More secure identity management systems combined with health information exchange services using a data centric data encryption approach and payment automation offer the prospect of greater security, enhanced privacy and over $4.5 billion in cost savings just from the widespread adoption of electronic payments. PayThat’s Payment System and PayThat’s Identity Assurance Federation (IAF) can achieve these efficiencies. For consumers, healthcare billing and Explanation of Benefits (EOBs) can be synchronized, eliminating the current system where consumers wait for the healthcare billing statements and EOBs to arrive separately before attempting to match them, prior to payment, and they frequently do not match because it is difficult and costly to reconcile data between the clinical data held by providers and the claims data held by health insurers and banks. Due to the efficiencies gained by health insurance companies from adoption of PayThat’s healthcare payments automation services, consumers can earn discounts on their health insurance from health insurers. Starting with a pilot implementation in Michigan covering 1.5% of the population the U.S., PayThat’s healthcare payments automation services will be adopted by other health information exchanges nationwide and ultimately roll out to the entire U.S. population and to mass merchants through their retail pharmacy operations. PayThat software and applications will achieve ubiquity.

Description of Business Opportunity & Implementation Plan

PayThat intends to provide single sign on (SSO) identity management and medical payments services to the health information exchange industry. The initial pilot customer would be the Southeast Michigan Health Information Exchange (SEMHIE), which is a non-profit collaborative of six major health systems that serve a medical trading area of 4.5 million, including half of the population of Michigan and 1.5% of all people in the U.S. SEMHIE’s
membership includes all other key participants in the regional medical ecosystem (health plan payers, physicians, trade associations, medical service providers, employers, quality organizations, safety-net providers, financial institutions and healthcare professional associations, including 14,000 Detroit area providers). By decreasing costs and improving the quality of care, SEMHIE has become a self-sustaining Health Information Exchange (HIE).

SEMHIE is providing seamless electronic access to health information from multiple large and complex providers each with disparate technology by deploying:

(i) Standards based approaches that are cheap, flexible, interoperable and repeatable;
(ii) a Service Oriented Architecture infrastructure that allows us to easily add business services for growth;
(iii) a common information exchange model for semantic interoperability.

SEMHIE’s near term goals are to:
(iv) deploy standards-based digital credential solutions to automate the identity management process;
(v) implement a role-based access control approach and the use of attributes to facilitate identity and role in context to all shared medical data, validated by audit; and
(vi) roll out services for four targeted use cases, discussed below.

PayThat can provide the identity management, role based access control and healthcare payments related services as an implementation of the proposed Identity Assurance Federation and PayThat Payment System under contract with SEMHIE. Other HIEs across the United States require this service and there is no other credible competing service available today. The incumbent payment system in the healthcare sector is the paper check.

SEMHIE’s Infrastructure is built on a cloud/SOA base, and was the first cloud/SOA based HIE to become a member of the Nationwide Health Information Network (NwHIN). SEMHIE has a NIST validated CCD (Continuity of Care Document- a CCD is an XML document that contains medical history and clinical code data) which has passed conformance and interoperability tests with the HHS ONC NwHIN and is “GO LIVE”. This CCD has a section to populate payment data.

SEMHIE’s first SOA service is a Social Security Administration (SSA) Disability Claims service which was built under a $3 million contract with SSA, hosted on a CSC cloud with key integration assistance from CNSI and other key healthcare industry IT partners. This service, which successfully passed several key milestones, accelerates the time to achieve approval for a SSA Disability Claim from 457 days to 6 hours for an approval. The SOA Service collects the information to pass a complete medical history to SSA via the NwHIN. SEMHIE’s innovative architecture using a SOA infrastructure allows the cost efficient, recombination, mapping and reconciliation of clinical claims data (ICD 9, ICD 10 codes, SNOMED & LOINC) with Electronic Funds Transfer (EFT) Extended Remittance Advice (ERA) payment data.

Because SEMHIE’s CCD XML document enables the merging of clinical data with payments related data it is possible now to break down these two silos and revolutionize medical
billing and presentment of Explanations of Benefit (EOBs), which detail what medical services are covered by health insurance and what medical services must be paid for by consumers.

Banking industry research indicates that payment and remittance processing costs an average of $11-13 per payment. Using EFT and ERA the cost could be reduced by 71-77% to $3.08 to $3.30 per payment. With adoption these savings would accrue to healthcare providers and healthcare insurance firms.

The current service and three planned additional services across four planned use cases can be made more secure and made widely accessible via the internet if a strong security management solution incorporating Federated Identity Management (Single-Sign On) is added. By partnering with PayThat, SEMHIE will be able to create a trusted computing environment to protect and encrypt the data of a personal health record and provide for the confidentiality, integrity and availability of the data based on role, authority, authentication status and need to know. By architcting a standards based solution and implementing a "data-centric" approach, SEMHIE’s service shall encrypt and "tag" the discrete elements and values with multiple strength levels of encryption and encapsulate the messages as appropriate and enable this information to be accessible via the internet while still preserving confidentiality, integrity and privacy.

Encryption is currently not ubiquitously deployed in healthcare but needs to be. More personal privacy protected information data breaches occurred in healthcare in 2015 than any other industry. HHS is starting to levy large fines for data losses. SEMHIE will provide for access control through the use of the IAF and Digital Credentials, and is standards based with the NIST 800 series and FIPS 140-2 as the primary approach. SEMHIE’s work will utilize the NIST Cloud Standard, NIST SP-800-145.

SEMHIE’s approach will use the Identity Assurance Framework which the National Strategy for Trusted Identities in Cyberspace (NSTIC) program has adopted as a core principal to ensure the Internet is more secure going forward. Strong "Federated" Identity Management is a basic requirement to make HIPAA protected healthcare data widely available via cloud based SOA "services“, such as what SEMHIE’s cloud SOA infrastructure uses.

SEMHIE shall create business activity with four use cases. SEMHIE’s member community shall enable ongoing input to define specific usability and user-centered design as the services are designed and deployed. The SEMHIE pilots are anticipated to become ongoing HIE services to the 4.5 million people in the Southeast Michigan medical trading area ecosystem. Starting with a pilot implementation in Michigan covering 1.5% of the population the U.S., PayThat’s healthcare payments automation services will be adopted by other health information exchanges nationwide and ultimately roll out to the entire U.S. population and to mass merchants through their retail pharmacy operations. PayThat software and applications will achieve ubiquity.
1. Single-Sign On (SSO) Use Case

With Single-Sign On you can access secure information on multiple participating internet sites without having to log on to each server. A Nurse or Physician can do e-prescribing, enter data into an EHR and retrieve data from a health plan to confirm health plan billing requirements all inside the same internet session without logging into or providing any security credentials at each site even if that data is resident at three different secure sites. Single-Sign On and Data Centric Encryption are both key requirements to having HIPAA protected data resident in a SOA/Cloud infrastructure and accessible to authorized users at multiple health systems in a complex medical trading area, such as Southeast Michigan. The wide deployment of a NSTIC Identity Assurance Framework would accelerate the deployment of these solutions nationwide and increase their usefulness. SEMHIE’s PayThat IAF enabled SSO service shall support a multiplicity of security authentication technologies (e.g. smart card, OTP, SAML, mobile devices, biometrics) because the medical provider ecosystem in which it operates has many legacy solutions deployed already for user authentication. SEMHIE shall adhere to the Fair Information Practice Principles as part of its governance framework, which shall be based on the Identity Assurance Framework of the Kantara Initiative.

2. Transitions Of Care (TOC) Use Case

South East Michigan Health Information Exchange (SEMHIE) is piloting ONC’s Transitions of Care discharge summary use case. This enables hospitals to discharge patients and provide necessary clinical data to the physicians who will care for the patients following release. Real-time, secure, authorized exchange of patient information in standard CCD format between Health Systems and Physicians EHRs - via SEMHIE’s Nationwide Health Information Network gateway service - will replace email and fax transmissions, meeting HHS’s meaningful use criteria. Semantic transformation of clinical data provides standardization for meaningful exchange of health records. The goal is to improve continuity of care and healthcare outcomes while decreasing costs. SEMHIE uses SOA/cloud and CONNECT infrastructure coupled with standards-based open software developed under its SSA e-Disability Claims contract. Using the PayThat IAF, SEMHIE shall expand the deployment of this Use Case throughout its medical trading area and overcome hurdles to achieving identity management and digital credential interoperability.

3. Payments Use Case

SEMHIE has a NIST validated CCD which has passed conformance and interoperability tests with the HHS ONC NwHIN. This CCD has a section to populate payment data. We will be conducting payments pilots to test and validate ways to achieve HHS mandates around Electronic Funds Transfer (EFT), Payment and Remittance Advice (ERA) and Health Plan Identifier with the members of SEMHIE. The SEMHIE Payments Use Case entails automating
and merging the healthcare payments with the clinical data of a large Health Lab serving 5 of the 6 health systems that are members of SEMHIE. At this Health Lab, most invoices are paid by check and those that are paid electronically result in thousands of payments with no relationship of payment to cause for what it is being paid. While currently, this doesn’t cause financial losses for the Health Lab because it is owned by the health systems for which it is doing the work, significant operational difficulties are caused by this inability to automate and reconcile the payments data with the clinical data. The Centers for Medicare & Medicaid Services (CMS) adopted a rule that adopts the NACHA CCD+Addenda as the standard under the Patient Protection and Affordable Care Act (PPACA) for Healthcare Electronic Funds Transfers. By using the ACH CCD+Addenda we can automate the paper process. Because the EFT and ERA rules mandate adoption, it is possible for this pilot achieve 100% adoption rates in providing this service in the clinical offices that use the pilot technology. The new standards are estimated by HHS to save up to $4.5 billion off administrative costs for doctors and hospitals, private health plans, states and other government health plans over the next 10 years.

4. Real-time Co-Pay Calculation and Collection Portal, Leveraging Real-Time Claims Adjudication Services Use Case

This will allow providers to dramatically reduce bad debt and eliminate paper billing and collections. This will coordinate with electronic EOBs (Explanation of Benefits). At check-in at a medical provider, a patient is provided with a written estimate of the cost of the service and what they will pay personally. The patient’s health insurance card will identify their provider, their health plan, and when “swiped” it will be used to determine deductible, co-pay and remaining deductible. A strongly enrolled mobile device containing a digital credential shall be used as an alternative method of validating the identity of the patient and their health plan. Eligibility and claims status inquiry can be resolved in real-time with an average response time of less than 20 seconds because HHS requires that all health plans that are CAQH CORE certified support real-time eligibility and claims status inquiry and response. At check-out at a medical provider, a patient is provided with a written statement of the actual cost of the service. Payment is collected electronically from the patient’s preferred payment method as selected in their PayThat CashBox. The electronic statement of benefits and final bill will be transmitted to the patient’s preferred device or email account. HHS standards make all this possible for 100% of the entire patient population that use the service at a medical provider that adopts the SEMHIE service. Consumer adoption of strong authentication technologies will be accelerated by this use case.

Financial Information

A detailed implementation plan requiring $2 million for Use Case #1 and $16.2 million for Use Cases #2, #3 and #4 was prepared, of which $1.3 million of preliminary work has
already been funded, completed and put into production for the initial SSA Disability Claims use case. Therefore, a total of $16.9 million of funding is required to build out the four use cases.

**Ongoing Adoption Plan**

SEMHIE and PayThat will work with the Michigan Health Information Network (MiHIN) to offer the piloted use case services state-wide. MiHIN is architected using the same “network of networks” approach used by SEMHIE and PayThat for its PayThat Clearing Banks. MiHIN shall develop a real world demonstration of a Use Case around providers and their staff accessing the variety of physician portals available to them.

**Risks to Adoption Plan**

SEMHIE shall collaborate with MiHIN to solve two challenges. One challenge is key management protocols do not interoperate across networks. The second challenge is that different vendor identity management solutions do not interoperate across networks. The whole goal of NSTIC is to develop a common business model for key management and digital credential vendor solutions to interoperate. OASIS does have a Key Management Integration Protocol Standard. We need to test this OASIS standard with constituents from the public and the private sector industry groups. MiHIN would also validate the network of identity providers for patients, providers, payers, school-based individuals, banks, and the State of Michigan employee users so that the identified set of relying parties can trust the credentials provided. MiHIN in collaboration with SEMHIE and PayThat could serve as the Identity Assurance Framework governance body for the healthcare industry vertical.

**Value Proposition for each class of entity:**

**The benefits for healthcare providers:**

- Verifying and collecting the patient liability at time of service for every visit reduces bad debt and collection costs.
- Better estimate of patient responsibility at the time care is delivered.
- Better estimate of patient responsibility prior to the time care is delivered.
- Reduction in patient frustration around the uncertainty of their benefits and amount owed.
- By supporting electronic claims status inquiries and responses:
  - Less staff time spent on phone calls and websites
  - Real-time claim adjudication can become highly supported
  - Exceptions can be addressed more timely:
    - Pre-adjudication acceptance or rejection appeals
- Incorrect or incomplete claim repair
- Information on why claims are suspended or not being adjudicated and what information is requested to complete processing of them
The benefits for healthcare insurers, including CMS (Medicaid and Medicaid, the largest health insurer in the U.S.):

- Healthcare billing and Explanation of Benefits (EOBs) derived from clinical data can be synchronized, eliminating the current system where healthcare billing statements and EOBs frequently do not match because it is difficult and costly to reconcile data between the clinical data held by providers and the claims data held by health insurers.
- Banking industry research indicates that payment and remittance processing costs an average of $11-13 per payment. Using EFT and ERA the cost could be reduced by 71-77% to $3.08 to $3.30 per payment. By offering consumers part of these savings from healthcare payments automation (merging the EOB with payment at time of service and making the EOB fully electronic), they can entice consumers with a discount on their monthly health insurance costs to provide continuously updated bank account settlement information to support straight through processing (STP) to determine deductible, co-pay and remaining deductible payment information.

The benefits for consumers

- Healthcare insurers will offer consumers part of the savings from healthcare payments automation (merging the EOB with payment at time of service and making the EOB fully electronic), by providing consumers with a discount on their monthly health insurance costs to provide continuously updated bank account settlement information to support straight through processing (STP) to determine deductible, co-pay and remaining deductible payment information.
- Consumers will no longer have to match and reconcile EOBs with healthcare provider billings for amounts they are alleged to be the responsible party for deductible, co-pay and remaining deductible payments. EOBs and healthcare billings will always match because the Healthcare billing and Explanation of Benefits (EOBs) derived from clinical data can be synchronized, eliminating the current system where healthcare billing statements and EOBs frequently do not match because it is difficult and costly to reconcile data between the clinical data held by providers and the claims data held by health insurers.

The benefits for technology providers

- Vendors will be paid fees for services provided in building and assisting day to day operations of SEMHIE, PayThat’s IAF, The PayThat Payment System and the PayThat Clearing Banks.

The benefits for processors (Depository Institutions & PayThat Clearing Banks)

- PayThat Clearing Banks and Depository Institutions will earn float income on all blocked good funds deposits held by the PayThat Clearing Banks.
• PayThat Clearing Banks and Depository Institutions will earn fee income for all payment services that carry contextual data
• PayThat Clearing Banks and Depository Institutions will earn fee income for all value added services

The benefits for PayThat
• PayThat will earn a royalty on float income and fee income for all payment services and all value added services

Stephen Lange Ranzini will be lead for PayThat. Mr. Ranzini, President & CEO of University Bank, which manages $18.5 billion in assets, is a recognized national and international expert in financial services standards development including Internet-based payment and data interoperability systems that incorporate federated identity management web services. Currently, he is a member of the Federal Reserve’s Faster Payments Task Force and a member of the Steering Committee of the Federal Reserve Secure Payments Task Force and a participant in the Federal Reserve Remittance Coalition, a select group of industry experts which is automating check payments.

Michael Talley will be lead for SEMHIE. He is the Program Manager for the SSA eDisability Contract for SEMHIE where he is Treasurer and a member of the Board of Directors. Mr. Talley is an approved ARRA Program Manager. Mr. Talley was invited to participate in the ONC/NwHIN Security & Privacy Sub-Workgroup and the Technical Committee and Security and Privacy Workgroup for the Michigan Health Information Network. Mr. Talley was the lead for the Affinity Workgroup for Security & Privacy for the HHS ONC HIE Beacon Communities.

Mr. Ranzini and Mr. Talley were actively involved founding members in the eAuthentication Partnership (k/n/a Kantara Initiative), and helped create and edit the Identity Assurance Framework.

Targeted Use Case #2: Email Spam & Fraud Prevention

Problem Statement

Due to the rapidly escalating threats to bank network security arising from criminal organizations, such as the Locky crypto locker software deployed by the Russian hacker gang Dridex, it is doubtful that continued usage of SMTP based email web services by Depository Institutions is actually compatible with the future safety and soundness of those Depository Institutions. All it takes to infect a bank network is for one employee out of hundreds, thousands or tens of thousands, depending upon the size of the Depository Institution, to click on a malicious email to infect the bank’s entire network, cryptolock the network accessible files and bring down the bank. While the current Locky crypto locker software is a virus and cannot itself jump from server to server within bank networks, making it reasonably manageable by FFIEC compliant banks, if the hacker gangs continue the research and development and deploy a worm version of CryptoLocker software, it has the risk of taking down entire banks. Since even the
best banks cannot get the failure rate by employees to avoid malicious social engineering attacks under less than a 1% per year frequency, and typical well trained bank employees fail well constructed social engineering attacks at over a 20% annual rate based on internal audit results, it is just a question of time before disaster strikes the banking industry.

**Elevator Pitch**

PayThat will move the banking industry away from standard risky email to “First Class Email”. Under First Class Email, no unauthenticated email will be presented to email users. All malicious spam will be blocked at the First Class Email SMTP gateway. PayThat will establish a bank-centric anti-spam blocking network under the brand-name “PayThat”, PayThat’s First Class Email will deploy a bank-centric implementation of the SAML protocol for Federated Identity Management, IPv6, the TOR Network and new network rules to create a protected zone of the internet, where only authenticated users can send or receive email and where senders of all email must attach a valid, good funds, immediately negotiable electronic check in the form of a PayThat Token in the amount of at least one U.S. cent. By substantially raising the cost of spam, the economics of the hacker gangs will be fatally undermined. As a major side benefit, the productivity of corporate workers will rise substantially as unwanted spam is eliminated from their daily routine and they will actually earn money to receive and read any unwanted First Class Email. Any identity related fraud related to First Class email will be investigated by the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal Service.

**Description of Business Opportunity & Implementation Plan**

The banks that participate in the network will benefit by making additional profits with little risk. Each clearing bank acting as a correspondent bank (PayThat Clearing Bank) would for a modest investment to purchase a license, own a fee driven business that would have a value of between $780 million and $1.30 billion at the end of the third year after product launch. Medium and smaller banks that offer the service through a correspondent bank would earn monthly fees per customer after paying the fee paid to the correspondent bank for providing the service.

First Class Email will require at least Level 3 enrollment and authentication to become an End-User and will utilize as a part of the enrollment process a web service that creates an email account with a .post.us top level domain. This has the result that any identity related fraud will be investigated by the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal Service. Also, through an existing treaty through the Universal Postal Union (UPU), any attempted or actual identity fraud in any of 190 member countries of the UPU, each of which have their own Postal Inspection Service law enforcement agency, is capable of being investigated by that country’s Postal Inspection Service law enforcement agency.
Email sent to a registered user by a non-registered user will move from server to server following the proximity mapping protocol embedded in the email standard Mail Transfer Authority (MTA) with each hop getting closer to the destination server. At some point along the route, the email will encounter an email server that enforces the new PayThat anti-spam network rule that the email must be from a registered user of the PayThat network and have attached to it a valid electronic check for at least a penny. At this point the email will bounce with an error message back to the non-registered sender.

The PayThat will provide the identity management services and micro-payment system to support First Class Email. The identity management services will be provided by the Identity Assurance Federation (IAF). The micro-payment system will be provided by the PayThat Payment System and PayThat Tokens. Because of the system architecture of the PayThat Payment System extra marginal transactions across the insecure internet actually have a zero cost, and therefore PayThat can be a profitable micro-payment system.

The Problem

For many years now corporations and individual consumers who use email have suffered from the problem of receiving unsolicited junk electronic mail (email), which is commonly referred to as "spam". The term "spam" was coined because it conveys the idea of receiving something that is undesirable, is of little or no value and similar to the meat product for which it is named after.

The Simple Mail Transfer Protocol (SMTP) email protocol is flawed in that it does not require identity management of either the sender or recipient of email, and the recipient of email pays for the vast majority of the costs of email. Being human nature to take advantage of the use of any resource that is free until that resource is fully absorbed, it is little surprise that over 90% of all email traffic consists of unsolicited advertisements from the senders of junk email ("spammers"). With the rapid increase of malicious criminal gangs who use spam email as a means for theft, looking forward, the uncontrolled Internet will become a toxic and much too dangerous environment for email if current trends persist. Proposals have been raised to modify and improve the SMTP standard, however there are challenges surrounding implementation, which information is available upon signing a standard Mutual Non-Disclosure Agreement.

The U.S. Congress responded to this threat with legislation against the spammers, however, the CAN-SPAM Act had the unintended effect of doubling the amount of spam because it made legal what was previously a grey area for business and the bill had some loopholes in it that really aren’t fixable. Truly effective legislation placing restrictions on senders of junk email would cost the U.S. government untold billions of dollars to even begin to attempt to enforce the legislation because of the relative ease and simplicity of spammer’s ability to operate their spamming operations outside (or inside) the physical confines of the U.S. in foreign countries where it would literally be impossible to trace let alone stop their efforts. A legal solution to email spam is not possible because a limited number of countries can be
financially incentivized to be bad actors, or even specialize in getting “shake-down” money from
developing nations while never solving the problem.

Because of currently available low cost technology and the simplicity with which
spammers can execute their spamming activities, spammers even now can setup spamming
operations anywhere inside or outside the U.S. at any number of physical (or virtual) locations in
a matter of minutes, conduct their spamming operations, and do costly damage to recipients of
their unwanted spam email messages. The spammers can then pack up their operations and
move to a different location or lay low in hiding until things cool down and they are forgotten
and later open up shop again under the auspices of a different name entirely.

It is estimated that cumulatively in the U.S., spam currently costs U.S. corporations
upwards of $20 to $80 billion dollars annually depending on whether the direct or indirect effect
is being measured. These costs are primarily due to lost worker productivity, extra computer
hardware, software licenses, bandwidth and personnel resources to handle the extra load spam
imposes, shifted management priorities to handle the spam, worker lawsuits when offensive or
pornographic spam is received, unwanted products being shipped, and worker confusion when in
doubt as to how to handle certain types of spam. There is also the psychological and emotional
toll taken by workers receiving unofficial health warnings or security warnings instructing them
to “act upon immediately” by the spammer, phishing attempts, where spammers attempt to steal
the identity of email users, successful identity thefts, the potential loss of their job if they open a
malicious email and the list goes on and on.

Computer viruses and worms are also primarily proliferated via spam email attachments
thus sometimes causing permanent loss of data to the unsuspecting spam recipient. Spam is also
the primary vehicle used to contact and ensnare potential victims in “web site fraud”. The
spammer might send an email to their victims instructing them to visit the spammer’s web site
while the spammer’s web site pretends to be the real web site of a famous company like
“Discover” credit card services, “WalMart”, “EBay” or “Amazon”. Criminal networks and
terrorists have used this technique to steal billions of dollars, and the rate of loss is increasing
geométrically according to the FBI.

It is in particular the phishing problem that has attracted the interest of the banking
industry to solving the email spam problem. Several major banks have sustained substantial losses from phishing activity. Victims have included customers of Citibank, eBay, PayPal,
Wachovia, Bank of America, Visa and Wells Fargo, all of whom have publicly warned of phishing attacks. Scammers even have used phishing emails to victimize two top government
and industry bigwigs, the Federal Deposit Insurance Corp. and the American Bankers
Association. The FBI, itself a victim of phishing, denounced it as “the most troubling new scam
on the Internet.” Most recently, the Central Bank of Bangladesh lost $105 million from its
account at the New York Federal Reserve due to a spearfishing attack against its SWIFT
credentials.

However, in order to address this problem effectively banks have concluded that they
cannot do it alone. They must have the cooperation of the Internet Service Providers (“ISPs”) to
help to address the problem effectively. The ISPs care about spam because it absorbs resources,
increases costs and causes users to discontinue ISP service. If the banks can address spam and
not just phishing they will get the cooperation of the ISPs. Some Telcos benefit from transmitting spam so you must have the ISPs assistance to solve the problem because the Telcos won't necessarily assist with infrastructure changes. If the banks address spam and not just phishing they will have the business case to get the money to do this, whereas if only a solution to phishing is pursued, there is no guarantee that a business case for either the banks or the ISPs can be developed. The banks have concluded that the solution must go to the root of the problem and not just be reactive or band-aids. The banks have concluded that the solution must be global in scope and not just not on law enforcement because law enforcement is not willing to be proactive unless a large theft of money is involved. The banks have concluded that the problem is lack of authentication of the sender of the email. The solution must therefore address the lack of authentication of the sender of the email. If the ISPs can easily block unauthenticated email the problem goes away. If the solution addresses the spam problem the money is there to build the business case.

If ISPs can reduce spam traffic, they can reduce the cost of providing email connectivity to their clients, and use less bandwidth, fewer servers and spend less money on spam generated security issues. The decreased costs will greatly decrease their operating costs and greatly increase their profitability. The role for ISPs in this environment can also be as supportive players to banks that outsource the email functionality of the bank-centric anti-spam blocking network or harmonize with them for security purposes. The bank-centric anti-spam blocking network itself, or one or more banks, may form a strategic partnership with the large ISPs.

**Description of Business Opportunity & Implementation Plan**

It is a well known fact that the primary motivation for spammers and virus authors to use email as a “transmission medium” is because using email not only provides a certain level of anonymity but also because it costs them nothing to do it. Their risk is virtually nothing. After paying their initial internet access fee or email subscription fee, they can freely send as much junk as they want without incurring any cost whatsoever. But, if it were to cost them something, they would certainly think twice about sending it.

Therefore the solution is to provide a software-based solution that is well regulated and managed by its commercial providers. It would be regulated and managed much like a Service Level Agreement (“SLA”) for application service providers. A solution that allows the recipient of email to clearly specify whether or not they wish to receive email from some or all sources or types of sources.

Using the PayThat Payment System, PayThat Clearing Bank “network of networks” approach, the IAF and Global Payment Gateway (GPG) technologies small incremental micro-payments ranging from a fraction of a penny to about $10 can be achieved cost effectively. A significant opportunity exists for users, both individuals as well as corporations, to reduce the volume of email spam while earning substantial revenue by implementing PayThat’s First Class Email technologies. Utilizing PayThat, the IAF and First Class Email, any recipient of email that is registered with the network can enforce a network rule that all incoming email must contain an electronic check for at least a penny that settles through the network. Since the response rate to
email spam is much less than 0.0001% of all outgoing emails, it will make it uneconomic to send spam email to protected email users.

Much in the spirit of “1-900” telephone numbers, the recipient would be able to actually charge the sender for the right to send them an unsolicited email or not charge them. The decision would entirely be left up to the recipient. The price charged would optionally either be set at the PayThat network minimum of one cent, or at an optional higher amount that could be set by the recipient at any amount above one cent (one dollar, one hundred dollars, etc.) or could be negotiated automatically or manually by the recipient’s preferences as established with the PayThat software with minimum and maximum limits set by either the sender, receiver, or both in either the initial software installation and setup or as reconfigured at any time thereafter giving flexibility to both parties. The recipient would never be allowed to exceed the financial limit set by the sender however, if they wanted to exceed the limit they would only be allowed to accept the maximum limit specified by the sender or choose not to receive the email altogether.

It is important to note that Persistent Digital Security software will have to be part of any solution that moves money securely over the internet. Also, that it is only with Persistent Digital Security software that client side solutions can be secure enough to be relied upon. With Persistent Digital Security software, whoever uses the software, for what purpose and based on what rules or policy can be tightly controlled. Access to the software can require authentication and digital checks can be transmitted over the open internet without fear that if sniffed or intercepted, that they can be altered without great expense of time and money. Master account holder profiles can be established and are architected into the solution, so that a head of household or a head of a business unit can delete access and account authorities as desired. The software is architected so that users can switch between multiple accounts in a single online session. While Microsoft and Phillips, which purchased PDS pioneer InterTrust, are leaders in Persistent Digital Security, it may not be required that licenses or coordination with their own Digital Rights efforts will be required since payThat’s Intellectual Property (see below, “Intellectual Property”) may be sufficient to avoid closer involvement of these organizations, if that is not desired from a business perspective. The use of Persistent Digital Security at the core of the bank-centric anti-spam blocking network software allows the following functionality which may not be achievable economically any other way:

- **Privacy Enhancing**: the use of Persistent Digital Security technology allows data to move freely throughout the Internet “cloud”, yet protects data from misuse due to rules based access and control of that data. The rules cannot be separated from the data ensuring compliance. Most databases do not utilize data-centric encryption, therefore traditional systems cannot ensure security and compliance. Traditional systems such as credit card and bank payment systems are as weak as their weakest node. With millions of Internet connected consumers and businesses the security problem is insurmountable with traditional database security systems.

- **Platform and Device Agnostic**: PayThat messages can move across and are compatible with all platforms such as PC, iPhone, GSM, G3 & G4 Cellular, Smart Cards, Bluetooth, IEEE-802.11 (a, b or g), or Legacy Systems.
Scalability: The single standard user interface can be used for micro-transactions, person-to-person, business to consumer, business-to-business and even government-to-government transactions and the system can also be deployed using any foreign currency. Users can be both off-line and on-line, increasing usability of the system.

Rjindael Compatible: Security protocols will be based on an open standard encryption protocol. One option would be to use the Advanced Encryption Standard (AES), an encryption standard adopted by the National Institute of Standards and Technology for the US government, as the standard encryption protocol. AES uses the Rjindael algorithm. The actual message layer protocol will not be open or published for security reasons and will be changed frequently among various standard configurations to further increase security. Using an open standard encryption protocol greatly enhances security.

Security Agnostic: PayThat is security method agnostic, because the sender of the email chooses the authentication security routine to be used for authentication purposes from the list of those routines supported by the sender’s financial institution’s policies. Multiple and/or successively more robust security policies may be supported or enforced depending on the preferences of the sender, the receiver, or both parties involved. Privacy templates adopted by End-Users can enforce these preferences on the data that relates to them.

Liberty Alliance, FAST & NSTIC Compatible: Since PayThat is security method agnostic, authentication capabilities will be compatible with the Liberty Alliance standard, NSTIC and the Financial Services Technology Consortium’s (FSTC) Financial Agent Secure Transaction (FAST) model for on-line authentication. The use of Persistent Digital Security allows the PayThat network to be compatible with whatever emerges as the banking industry’s preferred method of network authentication methods.

Open Standard: PayThat is designed with an open structure where API’s, ERP standards and cryptographic formulas will be published. An open standard will speed industry acceptance.

Viral Marketing: The basic PayThat program, the “CashBox™”, is sent each time a payment instruction is sent. Each email from a registered user will be sent with the required attached payment message, and emails can be sent to any email or SMS (mobile text) address. A recipient who is not yet a user can instantly become enabled to use PayThat by opening the message’s file attachment. A new user who receives a “CashBox” only then has to enroll with their bank to become a registered PayThat user. PayThat is self-distributing software, a method called superdistribution or viral marketing. Users will be protected from scams with a fast, simple, but effective method of reliably identifying whether an email payment they receive is legitimate or not via an authentication website run by the PayThat IAF.

Control Enhancing: The use of PayThat increases control of behavior and assures compliance with policy. Corporations or heads of households could use PayThat to enforce rules and policies and set variable authorities on demand. PayThat creates an easily auditable transaction trail.

Non-repudiation: PayThat can settle transactions in real-time. Credit card and ACH based payment systems allow up to 90 days for repudiation and dispute initiation. This timeframe is completely unrealistic for the needs of everyone for finality of payment.
Compatible with Government Rules and Regulations: PayThat was architected following extensive consultation with various government agencies. PayThat is fully compliant with the many needs of government in the Internet payments arena, including banking regulator, law enforcement and intelligence agencies. PayThat is compliant with all laws and regulations. Many of the non-bank-centric payment solutions being innovated will not survive because government regulation and laws inhibit non-bank systems from gaining traction in the marketplace. Banking regulators are against any non-bank payment system becoming successful because that would threaten their control of the payment system and the banking system and may be prompted to change the laws and regulations to protect bank-centric payment systems that they supervise from non-bank payment systems. These benefits that flow from the use of Persistent Digital Security are too large to ignore.

Anti-Spam Blocking via Micropayment System Preferred Implementation

We propose to establish a bank-centric anti-spam blocking network called “First Class Email” under the brand-name “PayThat”. The PayThat Payment System implements added email network rules to create a protected zone of the internet, where only authenticated users can send or receive email and where senders of all email must attach a valid, good funds, immediately negotiable electronic check in the form of a PayThat Token in the amount of at least one cent.

Email sent to a registered user by a non-registered user will move from server to server following the proximity mapping protocol embedded in the email standard Mail Transfer Authority (MTA) with each hop getting closer to the destination server. At some point along the route, the email will encounter an email server that enforces the new PayThat anti-spam network rule that the email must have attached to it a valid electronic check for at least a penny. At this point the email will bounce.

The sender and receiver of email would both be required to be enrolled users of the PayThat Identity Assurance Federation (IAF). The PayThat IAF is a bank-centric implementation of the Liberty Alliance SAML protocol for Federated Identity Management. Users would be authenticated by their own preferred and participating bank at time of registration and on an ongoing basis using Persistent Digital Security software incorporated into an applet that resides either at the user’s local client or at an email web service. Each bank that participates in the network would provide assurance of identity and that assurance would pass from the bank to embedded codes in the Persistent Digital Security software. The codes would indicate which bank authenticated the user and the method that was used by the bank to authenticate the user (e.g. internet banking login, biometric or other cryptographic method). Future access to the client side software applet Persistent Digital Security “Cash Box” is based on the authentication methods required by the bank that registered the user and made available by the bank to the user. Optionally, the bank could outsource this service to the IAF.

Only enrolled End-Users and Participants of the PayThat Payment System and IAF would be able to send email over the network to their intended destinations. Likewise, only paying customers of the PayThat network would be able to receive email from the network, thus providing the ability to filter 100% of all email messages they receive. Each subscriber or
customer of PayThat would also be known to the PayThat IAF as well as they are known to their own personal or corporate banks thus giving a high level of authentication of the identity of the sender as well as the receiver.

Here’s how a typical scenario would work:

Email sent to a registered user by a non-registered user will move from server to server following the proximity mapping protocol embedded in the email standard Mail Transfer Authority (MTA) with each hop getting closer to the destination server. At some point along the route, the email will encounter an email server that enforces the new PayThat anti-spam network rule that the email must have attached to it a valid electronic check for at least a penny. At this point the email will bounce back to the server or origin with an error message that reads:

This email has encountered an error because the intended recipient is a member of the banking industry’s anti-spam blocking network, PayThat. To learn more or to join the network, click on the following link, or go to www.paythat.net or www.paythat.com.

If they follow the link, this will take the individual to the main paythat.net or paythat.com web home page where they will receive a message “Welcome to the banking industry’s solution to the email spam problem. Please select the bank that you wish to register with.” Registration will actually occur at the PayThat registration server located at each bank’s website, or, if the bank has opted to outsource the authentication and federated identity management to IAF, at the default IAF location, or a PayThat Clearing Bank, at the default PayThat Clearing Bank’s location. Individuals who wish to register but whose bank does not participate in the network will also be transferred to the default IAF location for enrollment. Based on rules previously negotiated, the IAF will forward these customers to a default bank or authentication service provider for enrollment.

At the time the End-User is enrolled, they are prompted to download money ($5 to $10) to their “CashBox”, the client side software applet. This money is in the form of PayThat Token digital echecks and the funds are drawn from a user’s bank account at the user’s bank. Each time a user sends an email, the client side software applet automatically attaches a digital check in the amount of a penny, unless the user opts for a larger amount to be sent either automatically or manually. If funds are exhausted in the “CashBox” additional funds may be transferred into the “CashBox” from the user’s account at the user’s bank. The “CashBox” automates the replenishment of funds from the user’s bank account to the “CashBox” when a preset level is established unless the user opts to disable this function.

Once enrolled by a bank as a member of the network, the user would then install the client PayThat CashBox or the server-based version of the Anti-Spam component (for web-based email) using an automated help wizard. The user would then have the option to configure their default settings. They can choose to filter none, some, or all of the incoming email by a variety of mechanisms and classifications and types, etc.
These email and message sources and types of sources would be either specifically or generally classified or both within the PayThat Directory of Synergistic Services. Businesses could choose to be registered in the Directory of Synergistic Services if authenticated by their bank, by listing the products and services the business offers, including by type or category. If users choose to filter email based on category (as defined and classified via the PayThat Directory of Synergistic Services) and select a setting that specifies that they don’t wish to receive a particular type of email, then non-selected emails won’t be sent to them at all (and therefore won’t waste their time or their computer’s disk space or their ISP’s or corporation’s mail server). Heads of households or Master Corporate Users could enforce filter rules for all email accounts under their control. Pornographic or drug related emails could therefore be automatically cashed out without being presented to a users’ email inbox. We anticipate that the PayThat Directory of Synergistic Services would be based on the UDDI or similar standard.

If a registered user sends an email to a valid email address of someone who is a user, the recipient has the option of opening the mail or not opening it. They also receive a plug-in to their email browser that is a button that is a “delete and collect the money” button, so you don’t have to open the email to delete it. The “would be” recipient of the email who is a registered user of the PayThat network clicks on a dialog box choosing to receive the email after seeing the monetary value (or money plus coupon, etc.) they could receive if they opt to open and read the email. If upon reception of the email they see that it is a Spam offer or they find it annoying or obnoxious (for example, an email from a known source such as a marketing newsletter that the user didn’t sign up for), they may charge the sender of the email by pressing the “Delete and Collect” button, or let the charge automatically expire if the sender is not a true Spammer. Socially, it is less likely that you will delete and collect the pennies from people that you know or are in business with, otherwise they will likely start collecting your pennies, with ensuing ill-will being generated over nominal amounts of money.

If an email from a registered user is sent to a non-registered individual, upon receipt that individual can open the file attachment attached to the email. This will load the basic version of the client side software applet including the “CashBox” and prompt the individual to register with the PayThat network, leading them to the home page of the network that welcomes potential new users, as described above.

Email users bring their email system into the protected area of the internet covered by the new network rule that in order to send an email to a registered user inside the network you must be a member of the anti-spam blocking network and must attach at least the minimum required valid electronic check to each email. You can join the network without moving into the protected zone if your ISP doesn’t support it and you don’t want to move your email traffic to a new ISP. That just means that you’ll have to follow the network rules of sending valid echecks out with each email you send, but you won’t be protected from spam. Alternatively a local software client could be installed on your thin client that would bounce back the email that isn’t compliant with the network rule, but while this would lower the clutter in your inbox this wouldn’t eliminate any bandwidth problems.
If a user doesn’t cash the echeck the first time that the email browser is opened (or within one week of it being presented) with the email presented for opening, the echeck cannot be cashed at a later date. This is to prevent moral hazard at a later date when you need lots of cash and have thousands of uncashed emails stored on your email server! If you open the email the first time it is presented in your browser you can still collect the money by clicking on the “Collect and Delete” button, or just the “Collect the Money” button. Once you exit the email browser all uncashed echecks are cancelled and the clearing bank is notified, as well as the “CashBox” of the individual who sent you the email, which is updated with the new available balance available in their “CashBox” for sending echecks to reflect the fact that those echecks were cancelled without being cashed.

If a user wishes to, they may set a higher amount than the network default (say $100 when the network default is $1.00), or a lower amount (even $0.00) for a trusted counterparty (e.g. internal corporate email). As described in the documentation, a user may also establish an automated negotiation to establish the email “transaction” price.

If a user wishes to, they may opt to allow incoming emails from anyone in their address book, or just selected people in their address book, even if those people are not members of the spam-blocking network.

In a corporate environment, the sales department may wish to shunt all emails received by the corporation that are not from members of the network to a mailbox that is reviewed by less highly paid receptionists and clerks to ensure that no important inquiries from new potential customers are not lost. Similarly, the help desk may enable an account or series of accounts that accept all incoming email.

In a listserv environment, all members of the network when they sign up for the listserv will agree as part of the network rules that they cannot cash the echeck emails they receive from the listserv. If they wish to unsubscribe they must do so through the listserv and the network will enforce this rule by preventing the cashing of a digital check sent by a listserv to a registered user who is a registered member of that listserv.

Most consumers will probably receive more digital checks, stemming from email-based marketing pitches, than they themselves send. Therefore the typical consumer will likely accumulate money in their “CashBox”. At their option, a user can withdraw funds from their “CashBox” and transfer them to an account they hold at the financial institution with which they are registered. The fee will be small for withdrawals for next day credit and much larger for same day credit. Alternatively, excess funds can be emailed to a friend or business associate, or corporate account at no cost as a gift, to pay a bill or as use in micropayment purchases. Since spending money has no cost and withdrawing money has a cost, the PayThat network will make use of Gresham’s Law to its advantage. As stated in Gresham’s Law, the propensity will be for people to find ways to spend the money at no discount rather than to cash in the digital money and incur the exchange fee in converting the digital money to traditional bank account money. This means that an ever increasing amount of funds will be blocked in the PayThat Payment System and the PayThat Clearing Banks will earn an increasing amount of earnings from the float that earns interest income on those deposits.
Our Market

In order to be successful, the network must attract a critical mass of the following actors: large and small banks, ISPs, large corporations and mass market consumers. The bank-centric anti-spam blocking network (First Class Email) offers a Value Proposition to each constituency.

Value Proposition for PayThat Clearing Banks & Depository Institutions

The bank-centric anti-spam blocking network offers the following value propositions to banks:

- The banks that participate in the network will benefit by making additional profits with little risk.
- Each clearing bank acting as a correspondent bank would have an investment in a license and expense in establishing the PayThat Clearing Bank and a value of between $780 million and $1.30 billion at the end of the third year after product launch. Correspondent banks would increase the value of each customer enrolled in the network by a material sum.
- Medium and smaller banks that offer the PayThat service through a correspondent bank would earn monthly per customer fees less the smaller fee paid to the correspondent bank for providing the service. Medium and smaller banks would have a smaller but still significant increase in value per customer cross-sold the service. Medium and smaller banks can participate in PayThat on an equal access basis provided they can comply with all applicable PayThat Payment System rules.
- Banks earn money on increased float in the system. All customer funds loaded into “CashBoxes” are in non-interest earning blocked accounts.
- Banks earn money from fees charged to consumers to withdraw money from the blocked accounts to a regular bank account.
- Banks earn greater loyalty and closer relationship with customers;
- Banks can earn money by providing additional identity management services beyond the actual email spam blocking service described here. Risk management and risk mitigation are core bank competencies and if all customers were strongly authenticated additional web services could be sold on a fee for service basis.
- Banks have lower costs of serving consumers due to lower fraud losses and lower IT administrative costs due to a reduction in malicious viruses, worm, Trojans and phishing attacks.
- Smaller banks and medium sized banks can outsource PayThat services to a larger correspondent bank and make money providing this service while preserving and strengthening their customer relationships. A large number of smaller banks are needed for the system to be ubiquitous and successful because they have about half of the customer relationships in the U.S. In order to be successful and not to fall in the technology development chasm, the PayThat Payment System and IAF must scale up and
down and fit with the business models and IT resources of smaller banks, too. By offering smaller banks the opportunity to make money providing this service to their customers on a correspondent basis operating with the customer in the name of the small bank, the network meets the needs of the smaller banks also.

- Large banks can make money selling PayThat clearing bank services to smaller banks as a correspondent. It may be possible later for large banks to sell additional niche financial services to smaller banks and their customers via the PayThat network (see “Future Product Extension”, below).
- Banks of all sizes materially decrease the risk of cyber breaches by eliminating employee access to unauthenticated email.

**Value Proposition for ISPs**

The bank-centric anti-spam blocking network offers the following value propositions to ISPs:

- Decreased costs due to elimination of 60% or more of the network traffic that is pure spam prior to reaching their servers. The resources spent on connectivity can be reduced;
- Decreased costs due to elimination of viruses, worms and phishing attacks on customers. Substantial resources must currently be expended for security and customer service that will decrease;
- Increased customer satisfaction resulting in lower churn and higher retention;
- Increased profitability per customer.

**Value Proposition for WPPs and WHPs**

Web Presence Providers (WPPs) or Web Hosting Providers (WHPs) receive the following benefits:

- Decreased costs due to elimination of 50%+ of the network traffic that is spam prior to reaching their servers. The resources spent on connectivity are reduced;
- Decreased costs due to elimination of viruses, worms and phishing attacks on customers. Substantial resources must currently be expended for security and customer service that will decrease;
- Increased customer satisfaction resulting in lower churn and higher retention;
- Increased profitability per customer.
- New product & service offerings by joining our “PayThat VAR Program” for Value Added Resellers (e.g., offer PayThat “shopping cart” plug-ins, etc.).
- Provide greater variety of payment methods to “their” customers.
- New source of revenue streams based on a “per transaction” basis via special programs and incentives.
- New lead generation through subscriptions to “opt-in” mail lists.
Better, Faster, Cheaper “sign-up” for consumers
Improved payment tracking, monitoring, and reporting.
Greater reliability.

Value Proposition for Large Corporations

Corporations will join the network if only to gain the savings in cost and productivity that blocking out email spam offers. For example, a study at Daimler Chrysler concluded that the firm spends over $300 million a year on global email connectivity. Since over 50% of network traffic was identified as spam, if the spam can be eliminated before it reaches DCX’s servers and T-1 and T-3 pipes, over $150 million a year could be saved. The bank-centric anti-spam blocking network offers the following value propositions to corporations:

- Significantly reduced overhead costs by reducing the numbers of servers and network connectivity because spam never reaches the email servers.
- Ease of use for the Corporation staff
- Inexpensive for the users to implement, operate, and maintain
- Higher employee productivity and job satisfaction

Value Proposition for Consumers

The bank-centric anti-spam blocking network offers the following value propositions to consumers:

- Dramatic reduction of time-wasting and obnoxious spam;
- Consumers are paid for the spam they actually receive;
- Consumers can set the minimum payment amount at their desired level;
- No cost to the consumer, in fact they will make money over time from marketers who continue to annoy them;
- Ease of use;
- Ease of sign-up;
- Consumers inherently trust their banks and hence it is a natural sale.

Distribution Plan: Marketing & Roll-out Strategy

The solution requires banking industry collaboration and therefore the PayThat Payment System and IAF must be built and tested in a collaborative environment. The pre-commercial pilot will:

1) Perform initial testing & evaluation in a simplified environment;
2) Test a working prototype of the system;
3) Establish network rules and service level agreements (SLAs) for the participants while ensuring compliance with legal requirements;
4) Test a working commercial prototype of the system;
5) Prepare for and transition to the commercial launch of PayThat First Class Email.

Buy-in to the concept and pilot project will be made possible through a media strategy that includes placement of articles in American Banker daily newspaper and other banking industry publications such as Bank Technology News and in general Information Technology publications such as Information Week and other publications.

We have determined that the most effective way to cause rapid adoption is by creating pilot projects in partnership with mature well-established North American financial services companies and other large corporation. These pilot projects will immediately provide PayThat with large numbers of users and through "viral" marketing, the PayThat network will be spread quickly and cost effectively to all types of users, both in North America as well as Internationally. Since each large corporation has many suppliers and customers who wish to communicate with the corporation via email, the bounce back messages will create an impetus to join the network to continue these trusted relationships.

Roll-out Strategy to Banks:
Marketing to the masses of banks is proposed to be in partnership with the American Bankers Association. One of the key advantages of this business model is that it is not B2C but B2B2C, i.e., we are marketing to the 6,000 smallest banks through the bank marketing arms of the key bank trade associations, which in turn market to their existing client banks. This strategy will substantially lower the cost of sales and leverage the trusted relationship that already exists here. Although the initial reaction from ABA was favorable in concept, if a deal cannot be reached with them, we would approach the Independent Community Bankers Association instead with the same deal. We are familiar with the key personnel at both organizations. A key hurdle to overcome is that the banking industry is by its nature conservative to adopt new technologies. While getting the top 10 banks on board or many of the top 250 banks on board may be relatively easy, especially since they are highly motivated by the phishing and cyber security problem to act quickly, getting the masses of the 6,250 banks and 6,300 credit unions on board is a greater challenge. While the system will work if only a handful of the top banks sign up, it will be better and ease customer adoption if as close to 100% membership is achieved as possible.

Rollout of bank-centric anti-spam blocking network: The commercial rollout will probably happen in +1 year timeframe.

ABA would also partner to sell the banking industry the bank-centric anti-spam blocking network.

ABA's marketing machine comes at a cost - a % of revenues received is the traditional method. This would start at 10% and scale down as volumes rose.
University Bank already has a major endorsed product from the ABA. The American Bankers Association, through its Corporation for American Banking subsidiary, has exclusively endorsed University Bank’s subsidiary, Midwest Loan Services Inc., to provide residential mortgage subservicing services to member banks and their borrowers nationwide. Midwest is known for friendly, responsive service and industry-leading technology that help lenders retain customers, reduce costs and ensure regulatory and operational compliance. Midwest’s mortgage customers have 14x fewer complaints than the industry average according to the Consumer Financial Protection Bureau’s complaint database.

Roll-out Strategy to ISPs
Large ISPs will be recruited by a dedicated force of individuals working through the relationship manager at their primary bank. Since cost reductions and increased profitability opportunities are quite large we do not anticipate any foot dragging. Large ISPs will be actively recruited. Large ISPs who are early adopters may be offered some stock in PayThat or a profit earn-out as a further inducement.

Roll-out Strategy to Large Corporations
Senior management at large corporations will be approached by a dedicated force of individuals working through the relationship manager at their primary bank. A web based calculator will be developed to allow self-assessment of the potential cost savings that adoption of the network may offer in reduced costs and increased productivity.

Roll-out Strategy to Consumers
A list of identity theft victims will be either purchased from the credit bureaus or created from bank records. These individuals will be recruited as early evangelists. Articles will be written in the consumer facing publications to attract tech savvy early adopters. Articles will be written and press releases created to attract mass-market publications to write a story on the anti-spam blocking network to attract mass-market users. Banks that are members of the network will offer the service to their customers. Due to the viral nature of the network (each email from a member of the network is potentially a recruitment device) and the strong value proposition for consumers, it is hoped that rapid adoption of the network will occur. When the value proposition is compelling consumers will adopt new internet-based technologies. For example, skype.com offered its internet software based VOIP service and in less than six months attracted over 11 million users.

Business Model

Consumers will not be charged for the use of the PayThat CashBox and First Class Email and enrollment with the network will be at no charge.

Banks will earn revenue initially from two main sources:
• Earnings on float (all funds held in the PayThat Payment System blocked accounts will not be interest-bearing);
• Withdrawal fees (banks will charge a small withdrawal fee for next day withdrawal credit to the bank account of their choice and a much larger fee for same day withdrawal credit to the bank account of their choice)

Fees will also be assessed for customer service once certain benchmarks of adoption are reached. Customer service will be provided initially at no cost, and the concept of variable grades of customer service based on the profitability of each customer will be implemented as the system develops. Profitable customers will have better quality and free customer service, while unprofitable customers will have 900 telephone numbers and other methods (e.g. pay via PayThat Token echecks for email support).

By enabling businesses to link their systems to PayThat via an on-line e-Learning utility, PayThat avoids the model of one by one, direct sales in favor of self-service automation.

We anticipate that customer service will be centralized to reduce cost and that the business rules of the centralized customer service platform will strictly prohibit sharing of customer data among financial institutions or allow access to a second bank to a first bank’s customers’ data. Optionally, banks will be allowed to provide their own customer service, however, we expect that the cost of doing so will be less economic. As the customer base grows, two customer service centers of the centralized platform will be required, and ultimately, it is possible that to provide 24-hour, 7 day a week customer service, that overseas customer service centers will be established in different time zones.

Management

The proposed management team is:

Stephen Lange Ranzini, Chairman & President

Mr. Ranzini is President & CEO of University Bank of Ann Arbor, Michigan whose 347 employees manage over $18.5 billion in assets for over 115,000 customers nationwide. He played the leading role in the bank’s acquisition in 1988 when he became the nation’s youngest bank holding company President at age 23, a position he has held since. At that time University Bank had $34 million in assets and 21 employees and it has grown through the creation of niche financial services businesses. University Bank was selected as "Community Bankers of the Year" by both American Banker magazine and the American Bankers Association. For the past 5 years University Bank’s annual revenue grew an average of 22.7%. American Banker newspaper noted University Bank as the second most profitable publicly traded community bank in the U.S. based on its 18.75% annual average Return on Equity over the period 2012 to 2014.
and as the number one most profitable bank in 2015 based on its ROE of 25.2% and it’s ROA of 2.52%. University Bank’s five year average Return on Equity is 15.1%.

University Bank originated $721 million in residential mortgages in 2015, which were sold to the secondary market with guarantees from FHLMC, FNMA, FHA, VA, USDA-RD & FHLB MPF programs, and has originated in excess of $6 billion in mortgage loans sold to the secondary market under Mr. Ranzini’s leadership.

The American Bankers Association, through its Corporation for American Banking subsidiary, has exclusively endorsed University Bank’s subsidiary, Midwest Loan Services Inc., to provide residential mortgage subservicing services to member banks and their borrowers nationwide. Midwest is known for friendly, responsive service and industry-leading technology that help lenders retain customers, reduce costs and ensure regulatory and operational compliance. Midwest’s mortgage customers have 14x fewer complaints than the industry average according to the Consumer Financial Protection Bureau’s complaint database.

In addition to extensive experience in retail banking, mortgage banking, mortgage subservicing and Islamic banking, during his 27 year career as the head of University Bank, Mr. Ranzini has direct operational experience in the following additional areas: payment systems, retail securities brokerage, asset management, trade finance, asset backed lending, foreign exchange and venture capital.

In addition to his operational and management experience and skills, he has substantial IT experience, is the author of two fundamental internet security patents and as a participant of both the Federal Reserve Remittance Coalition and the Federal Reserve Faster Payments Committee, is considered a leading U.S. expert in payment system modernization. As a result, in July 2015 the Federal Reserve appointed him as one of only five bank executives nationwide to the Secure Payments Steering Committee, which is architecting the security architecture for the new Federal Reserve Real-Time Payments System. Prior to founding University Bancorp, when it acquired University Bank in 1988, Mr. Ranzini worked in the investment banking and money management industries.

A magna cum laude graduate of Phillips Exeter Academy, Stephen graduated from Exeter and Yale on scholarship and has served as both the President of the Yale Alumni Association of Michigan and as a Delegate to the Yale Assembly.

A Chief Technology Officer will be recruited and hired in Year 1 Month 1.

A Chief Operating Officer will be recruited and hired in Year 1 Month 11.

A Chief Architect, whose primary responsibility will be to assist the Chief Technology Officer and who will report to the Chief Technology Officer, will be recruited and hired in Year 1 Month 7.

A Chief Marketing Officer will be recruited and hired in Year 1 Month 2.

A Chief Financial Officer will be recruited and hired in Year 2 Month 7.
Other key officers, including VPs of Customer Service, National Sales and International Sales will be recruited on a hiring schedule presented in the Financial Projections.

An Advisory Board will be formally recruited.

A Board of Directors will be formed from the key strategic participants and investors in PayThat.

**Intellectual Property**

PayThat intends to license from Jove Corporation United States patent #7,120,606 covering 187 patent claims, filed on February 10, 2000. This filing dealt with the concept of a system and method for the secure electronic transfer of funds using email and Persistent Digital Security software, including Internet based payment networks that use Persistent Digital Security technology as a cash purse. The system is described as being device and security method agnostic.

PayThat intends to license from Jove Corporation a second United States patent #7,343,349 covering 106 claims, was filed on October 15, 2001. The second round of patent applications deals with five broad concepts:

(i) The concept of moving payments peer to peer via a Persistent Digital Security enabled secure system using email file attachments;

(ii) The concept of using the automobile to aggregate credit card transactions;

(iii) The concept of creating a personal portability profile that can be transferred between cars and possibly between cars manufactured by different firms;

(iv) Creation and use of XML compilers to speed up transaction rates for ERP enabled payment messages utilizing XML;

(v) Use of voice-centric payments network and voice-centric authentication method for the secure electronic transfer of funds using email and Persistent Digital Security software.

Additional major claims in the context of those five categories include:

1. Email based secure bank centric payment clearing network;
2. Open standard, email based secure bank centric payment clearing network with open standard cryptography;
3. Moving general ledger and ERP data along with payment data in those networks;
4. Using the FAST interoperability authentication process for managing multi-tier, multi-method, multi-user authentication technologies;
5. A directory of synergistic services (PayThat yellow pages)
6. A directory of users’ profiles and attributes (for trust brokering by PayThat clearing banks);
(7) A directory of aliases (PayThat white pages of PayThat users without needing to make your email address public);
(8) A help wizard in those networks;
(9) ERP wizard for integration of ERP systems to PayThat in a self-service environment;
(10) Network databases for: Customer Information File, Pending Transactions, Validation, eCheck Numbers, Authentication, Authorities, Audit, ERP;
(11) Integration of PayThat with an email browser (standard email software or custom software, device or voice based);
(12) Email clearing house that performs virus-checking, authentication, spam-blocking, hacking protection, denial of service attack protection;
(13) Privacy matrix using Persistent Digital Security software in those networks;
(14) Subordinate subscribers in those networks;
(15) Interfaces with on-line currency exchange in those networks;
(16) Variable expiration dates less than seven years or the legal escheat time limit;
(17) Bearer versus certified funds in those networks;
(18) Sender chooses authentication method in those networks;
(19) Intelligent agent for automating processing of business transactions;
(20) Setting an automatic minimum level for redeposit or refreshing of the “Cashbox”.
(21) eLearning Wizard system
(22) Econometric and law enforcement research process;
(23) Customer Service model for variable service levels based on customer profitability in those networks;
(24) Email diagnostic tool for customer service management;
(25) The risk control process in an email based secure bank centric payment clearing network;
(26) The message set process (order protocol and data set) and order of messages in those networks;
(27) Using the ATM POS system for settling irrepudiatable email based transactions in those networks;
(28) An Internet-based secure healthcare data exchange network system.

The work underlying patent applications #2 and #3 above have been architected into a working system around the business model described above, using Unified Modeling Language (UML) and Model Driven Architecture (MDA).

These patents have been cited as prior work in patents issued by VISA, AT&T, IBM, eBay, Nokia and Coinstar.

**Future Product Extensions**

Once built, the PayThat Payment System and IAF could be used by businesses and consumers for many additional functions. Essentially, PayThat has at its core a fully functioning
micropayment system. However, after assurance is gained via operational experience that the network is highly secure, larger payments could be made through the network. Since the network is TCP/IP based and XML enabled, it would be possible to move money (payment instructions) as well as associated data, including ERP data, via the network. This would lead to the creation of whole new industries and spin-off opportunities focused on specific vertical markets. These value added services would generate new sources of income for the banking industry and banking industry vendors.

To date, no successful micropayment system has been built. The first problem that must be overcome with any micropayment scheme is that you must overcome the Metcalf’s Law problem, or "Chicken and Egg" conundrum (in less scientific terms). If few people use the system, it isn't very useful, therefore you yourself won't adopt. If few people use the system, you can't pay many people with it, therefore it isn't very useful. Metcalf's Law says the same thing in a different way: the value of a network is equal to the square of the users of the network or the square of the functionalities of the network. Most existing micropayment schemes have been designed in such a way as to not interoperate with existing bank payment systems. Also, they must generate their own demand from micropayment activities alone. Any successful micropayment system must provide a level of interoperability with bank payment systems (because those networks have many existing users and therefore strong value). Email, as the most useful and used software and the internet, as the largest shared network, could theoretically provide rapid adoption and a rapid increase in usefulness, if a large initial user group migrates to the new system to seed it. There are at least four groups which have the large critical mass to successfully initiate this. The largest banks, with their millions of employees, have the critical mass to start this. The U.S. Government has the critical mass, the largest auto manufacturers (through the control of their supply chain on which 1 in 7 jobs in the U.S. depends), and the healthcare industry (the largest single U.S. industry), have the critical mass. One of these four groups or a combination of them would be required to adopt to kick start the creation of a large enough value network to ease the path of adoption and to create enough of a value proposition to overcome Metcalf’s Law.

Because the end result of the success of the bank-centric anti-spam blocking network is a fully functioning micropayment system any level of activity of micropayment processing across the network will be profitable. The success of Apple’s iTunes online store indicates that there is a demand for micropayment transactions, however, the iTunes store loses money on every transaction while making money selling iPod .mp3 players and iPhones. This is because using credit cards, a relatively expensive method to purchase songs, is too expensive for the economics of the online song store business:

$0.99 to Apple
- $0.60 to digital content provider
- $0.30 to credit card vendor
$0.09 to Apple (gross margin for support, marketing, overhead, profit (?)

© 2016 Federal Reserve Banks & University Bank. Materials are not to be used without consent.
There has been a lot of talk about deflation in the economy in recent years, however the most rapidly depreciating thing is the value of information. The internet has made people believe that most information is free. Therefore the perceived value of information is low. Because of convenience issues, consumers are willing to pay something for information if payment is convenient, however, they are not willing to pay very much. I might want to know what the weather is going to be tonight, but I’m not willing to pay $0.99 to know, and I might not even pay a penny to know. I might pay 1/10th of a cent to know.

The lack of a fully functioning micropayment system that interoperates with existing bank payment systems and bank accounts has been a substantial barrier to the success of many internet business plans. The business models of many web services are being blocked by payments. The lack of consideration given to how a consumer was going to pay for something where the service is provided online is probably one of the major reasons why the initial internet bubble burst. However, as stated, any micropayment network must overcome the Metcalf’s Law functionality problem to become successful, and no single information service is compelling enough to cause a micropayment system to develop. A fully functioning micropayment system that is built and funded for an entirely different purpose and is linked to tens of millions of frequent email users cuts through this problem quickly. Examples of micropayment based services that cannot catch on until there is a very low cost micropayment network available are:

- Multi-media Digital Data download
- Geolocation services
- Information content service providers
- Payment for mass media news articles

Beyond micropayments, many additional web services could be conceptualized that could take advantage of the PayThat network because it has the ability to move payments with data in an XML-enabled and TCP/IP native environment. We believe that Banks and other web service providers will be able to leverage the basic infrastructure of PayThat to sell services to customers of smaller banks, resulting in a larger pie to be divided. Fee income could be split among the banks by negotiation or network rules to be established to ensure the ability of banks of all sizes to provide PayThat services on an equal basis. We plan to take advantage of these web service opportunities following full development of PayThat, deriving licensing revenue from the sale of value-added web services by participating banks and web service providers. Since the network is built and paid for on an entirely different basis, even if these web services take a long time to catch on, it won’t matter. The economics of the basic business plan are sound and the returns compelling even without the additional services.

Financial Plan
Financial projections indicate that a network that can serve 69 million unique individuals (5% of the current worldwide email users) can be created with a $25 million initial capital investment.
Preliminary financial projections indicate that the PayThat network will be earning at a run rate in the 4th quarter of Year 4 of over $15 million earnings before income tax, or $62 million EBIT annualized, and the value of the company would be approximately $940 million to $1.55 billion.

Other key assumptions and details of the financial plan are available under MNDA. We are willing to share the following publicly:

1) The following personnel are required: Month 12 37 Full-Time Equivalent Employees (FTEs), Month 24 67 FTEs, Month 36 85 FTEs, Month 48 101 FTEs. Salaries are assumed to be at market rates with stock options for the board of directors, advisory board and key officer employees;

2) The proof of concept pilot equipment will serve as a pre-production test bed to test network upgrades prior to being released commercially. We assume that the commercial launch of the network will be on a second system that is built and put into place in months 10-13;

3) 10,000 ft² of office space will be required in Year 1, 15,000 ft² in Years 2-4. The customer service call center will be outsourced or offsite;

4) The network charges nothing to customers to load money into the system, but charges to withdraw money from the system, charges fees for foreign exchange transactions, and charges fees for valued added data enhanced transactions for businesses. The network earns float off money held in the network each day that the money is held by the network. Specific volumes and rates are listed in the “Revenue” worksheet;

5) The intellectual property required to build the network is acquired from University Bank, Jove Corporation, TecSec and Todd Sundsted;

6) Bank debt or vendor financing terms are required in Year 3 Quarter 3 and Year 4 Quarter 2 when large mainframe and network server purchases are made to expand the network’s capacity;

7) The network becomes cash positive in the 41st month after launch. The network becomes GAAP profitable in Year 3 Quarter 3, or 21 months after the commercial launch.

Financial & Operational Risks

a) Micropayment systems usually fail. No micropayment system has been financially successful. Over $5 billion has been spent in the past twenty years on micropayment system companies, however every project to date has failed because of the Metcalf Law or “chicken and egg” problem. Without widespread adoption and usability, the propensity to join the network will be low. Who is motivated enough to join the network even though the level of users of the network is low? We plan to deal with this risk because the bank-centric anti-spam blocking network attacks a different problem directly where there are many highly motivated early adopters, the micropayment system is a by-product of the solution and does not have to bear the cost of developing the system on micropayment fees. The PayThat Payment System and IAF are fully paid for before the first true micropayment transaction is made across the network.
b) e-Postage schemes have been proposed in the past but never get off the ground. One of the problems with past notions of e-postage or charging the sender that have been proposed in the past is that there was no effective way to settle the transactions through the banking system. The scheme would be technically feasible but impractical in the real world. If the postage can't be charged and settled cost effectively, someone would have to absorb the per transaction loss. In contrast, the PayThat network designers have put the time and effort into designing a business model that works as well as a technical architecture (incorporating Persistent Digital Security) that is secure and uses the open internet, it has no extra infrastructure cost (beyond the one-time upfront capital cost to build the network and software). Because the extra marginal transaction is theoretically close to free, it can be cost effective, as opposed to current bank payment systems. For example, the ACH system costs about $0.003 per transaction to transmit a payment instruction but this does not include additional overhead at both the receiving and sending bank. Plus there is essentially zero security (i.e. end user authentication) associated with this system (and as a result fraud losses from internet sourced transactions are rising). It would be unwise to marry the ACH system to an e-Postage system. All other existing bank payment systems are more expensive than a penny, also have major security flaws and have greater associated overhead at both the receiving and sending bank, so they also cannot be used as the settlement mechanism.

c) Scalability of the transaction engine at the core of the network. The third problem with such a system as we are discussing here is that the transaction engine at its core must be very reliable and must be capable of processing a lot of transactions (for example VISA Net processes more than 8,000 payment messages a second and this network would require higher velocity and capacity. To counter this risk, we have already given some serious thought to how to achieve the scalability needed, however, this is an area where some serious testing, validation and benchmarking will be required. Additional assistance with this issue will be required and we anticipate that NIST and some of our friends at the government labs will be able to assist us with that design, design validation and design testing (MDA/UML) process when we get to that point. The key here will be not just reliability and robustness, but a combination of robustness and cost. If the cost is too high or the per transaction cost of running the core processing systems are too high, the economics of the system break down quickly. Of course, it must be highly scalable and survivable. We can't have the system break down because of high usage or because of an attack.

d) Technology. If the technology doesn't work as advertised or isn't as secure, or the cryptographic methods underlying the payment messages is cracked, the network could lose money or fail. Competent management, backup crypto plans and Internet e-commerce insurance controls this risk.

e) Corporate user adoption. If insufficient corporate user acceptance occurs, the network will not gain widespread user adoption. This risk is mitigated by the system design which eases adoption by corporate users and by the value proposition of large cost savings, substantially increased cyber security and productivity savings.

f) Consumer user adoption. If insufficient consumer user acceptance occurs, the network will not gain widespread user adoption. This risk is mitigated by the system design
which eases adoption by consumer users and by the value proposition of potential income from receiving spam marketing messages and productivity savings.

g) Customer acquisition costs. If customer acquisition costs are too high, we will fail. Under the model users will not be charged to join the network and all authentication service providers will be paid out of network profitability. If the cost of user authentication is higher than planned this will require additional working capital investment.

h) Ongoing operating costs. If operating costs to run the transaction engine at the heart of the network, government compliance costs, or non-recoverable network operating costs or non-recoverable customer service are too high, we will fail. Initial monthly operating costs are estimated at $740,653 per month, excluding marketing costs of $1,000,000 per month. With 12,000,000 users, we estimate that the PayThat First Class Email service will be profitable. The business model mitigates this risk because cash is paid upfront in the stored value business model. If the network’s break-even point is higher than anticipated, we will run out of cash. Ancillary services and other use cases may become a major source of additional fee income, however they may take time to become established.

Value Proposition for Strategic Partners

Large Banks (Correspondent Banks)
Each clearing bank acting as a correspondent bank would have an investment in a license, and expense in establishing the hub and a value of between $780 million and $1.30 billion at the end of Year 3 after product launch.

Medium and Smaller Banks
Each financial institution that offer the service through a correspondent bank would earn monthly per customer fees less the fee paid to the correspondent bank for providing the service.

ABA or ICBA marketing arm
A fee equal to 10% of the revenue earned by the network per bank recruited into the network would be paid with a cap of $20 million per year, or a total of Year 1 $0, Year 2 $1.4 million, Year 3 $18.0 million and Year 4 $20.0 million.

ISPs
Profitability of ISPs would increase from approx. 8% of revenues to 30% of revenues as their cost of providing internet provisioning decreases, or an increase of 250% in the value of the enterprise OR, the extra profit could be placed into increased market share via lower connectivity fees to consumers.

WPPs and WHPs
Profitability of WPPs and WHPs would increase comparably to the increase in profitability of the ISPs as their cost of providing web services decreases, OR, the extra profit could be placed into increased market share via lower fees to consumers.
Large Corporations
Lower costs and productivity gains per employee are estimated to be $300 to $1,000 per employee, or $3,000,000 to $10,000,000 per year for a company with 10,000 employees and $30,000,000 to $100,000,000 per year for a company with 100,000 employees.

- The high cost of traditional filtering can be eliminated since it isn’t needed
  - First Class Email eliminates the need for traditional filtering
  - Bad messages bounce before they ever reach the destination mail servers
- Solves the problem of senior officers who are drowning in email
  - Network minimum is $0.01 however more senior corporate officers can set a higher minimum (e.g. CEOs $100, SVPs $10, VPs $1) so that the account of a “bcc” or “cc” abuser is quickly drained through instant feedback of taking the electronic check. Without requisition from a superior officer the email abuser cannot send email up or across the chain of command.

Marketing Firms
- PayThat makes possible more targeted advertising at a lower cost than U.S. Mail with greater effectiveness than spam email.
- New geolocation and proximity services can be enabled in the field:
  - First Class Email can be used in conjunction with GPS and email enabled smart phones to send new listserv messages such as residents@geo.xxxxx-xxxx.com or devices@geo.xxxxx-xxxx.com, where xxxxx-xxxx is a zip plus four zip code.
  - Send messages immediately to all participants who are in physical proximity by category or type through interaction of intelligent routing and GPS devices
    - E.g. devices@geo.xxxxx-xxxx.com would reach all enrolled devices within the specified physical proximity requested by the sender
  - Identity and addresses of the recipients are shielded from the sender
  - Response is at the sole option of the recipient

Consumers
The average consumer would gain $1 to $5 per month in net revenue from “First Class” email marketing solicitations they receive in excess of email postage they pay out.

Strategic Investors
Each $1 million invested is worth between $7,431,365 and $12,385,608 at exit in the 48th month after start-up per $1 million invested, assuming an exit at between 15x and 25x earnings before tax.
Targeted Use Case #3: Single Window for Cross Border Trade Facilitation & Supply Chain Billing

Problem Statement
To import or export goods into or out of the United States, signed documents must be procured from 33 different federal government agencies. This is an expensive, complicated and time-consuming paper intensive process. Most smaller manufacturing firms based in the U.S. are discouraged by these barriers from exporting. Exporting goods or services creates four spin-off jobs for each manufacturing job created, the highest such ratio of any industry type.

Elevator Pitch
The Single Window allows a firm that wants to export or import any goods across the borders of the U.S. the ability to obtain all the documents required by filling out just one intelligent web form. As the form is filled, intelligent options are presented based on the information provided. The list of “supporting” documents required to finalize the transaction is derived from the data in the declaration. At the end of the process, the End-User digitally signs the intelligent web form once and the required information, certificates and documents are prepared behind the scenes in an automated fashion by the various government bodies. Certificates and documents are created in real-time on-line and delivered in a secure electronic portal to the End-User by accessing the databases of the applicable government agencies. By greatly simplifying the process of obtaining all the documents required, more corporations will be able to import or export goods across the borders of the U.S. The Single Window earns fees for this basic service and from value added services offered through the Single Window to End-Users.

What is a “Single Window” and Why is it Very Useful?
World Customs Organization (WCO) defines a Single Window for Cross Border Trade Facilitation or “Single Window” according to Recommendation Number 33 of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) as:

“a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, export, and transit-related regulatory requirements. If information is electronic, then individual data elements should only be submitted once.”

In practical terms a Single Window environment provides one “entrance”, either physical or electronic, for the submission and handling of all data, and documents related to the release and clearance of an international transaction. This “entrance” is managed by one agency, which informs the appropriate agencies, and/or directs combined controls. The various Administrations integrate the processes within their competence (of which they are holders), thus offering a common “interface” to citizens and enterprises. With the data collected in the customs
declaration an Information & Communication Technology (ICT) process is triggered to check the documents supporting the declaration and to perform controls.

The World Bank estimates that countries average 73 documents per customs declaration, released by over 20 government bodies. In Italy, up to 68 documents must be released by 17 government bodies. In Australia 105 documents are required.

Over 30 countries from all regions of the world have introduced a Single window facility and have achieved considerable advantage through the reduction of time and resources in preparing, presenting and processing official information requirements. Single Window facilities often result in a decrease in trade transaction costs, improved trader compliance through more accurate and timely data submission with an associated increase in government revenues, and more efficient and effective border management and controls.

The Single Window consists of an intelligent web form. As the form is filled, intelligent options are presented based on the information provided. The list of “supporting” documents required to finalize the transaction is derived from the data in the declaration. At the end of the process, the intelligent web form is digitally signed once and the required information, certificates and documents are prepared behind the scenes in an automated fashion by the various government bodies. Certificates and documents are created in real-time on-line by accessing the databases of the applicable government agencies.

**Additional Valued Services Enabled by a Single Window**

The Single Window approach is key to reduced costs for enterprises that import or export. Other value added services can then be added to the Single Window, including valued added services such as the proposed i-Port Authority, an e-Logistics B2B Solution that allows all transportation companies to provide their services on-line, all the time. The resulting system would be capable of moving anything anywhere other than a person or a letter. It would be similar to an airline reservation system, but for all types of transportation, including air cargo, ships, rail, trucks and other logistics entities. Beyond the supportive services provided by the Single Window such as customs clearance, the proposed i-Port service utility would provide valued added logistics services, banking services, and trade finance services.

Services available on-line from the i-Port service utility in real-time would include:

- Confirm shipping costs (all billing could include total shipping cost)
- Instantly track shipments across carriers
- Rapidly evaluate alternatives when requirements change
- Predict shipment arrival in real-time
- Obtain real-time status of mobile assets
- Schedule loading dock personnel
• Know and authenticate the identity of all people involved in the entire logistics supply chain
• Settle payments globally in multiple currencies, with each transaction’s ERP data flowing seamlessly
• Make payments through secure, trusted payments environment
• Real-time dispute resolution including required rework of incorrect invoices

Status of U.S. Effort to Build a Single Window

President Obama signed an executive order in February 2014 directing the federal government to establish a “Single Window” to facilitate cross-border trade by December 2016. This is a large effort across 43 federal government agencies. South Korea, Italy and Australia are already up and running with Single Windows for trade facilitation. The U.S. Single Window will allow a business to fill out one online intelligent form that can be digitally signed to easily complete all the hundreds of forms required to export or import anything into or out of the United States. However, to date, the federal government effort to implement the Single Window is not focused on any business use cases or adoption strategies and has little functionality.

Possibility of a Michigan Pilot to Build a Single Window

There are huge opportunities for Michigan to be the pilot implementation site. If one of the Big Three put their hand up and said that they wanted to be the focus for a pilot based in Michigan, the initial nationwide implementation could be fine tuned to meet the needs of the automotive supply chain ecosystem. Having been the U.S. representative to the United Nations group that built this standard, I know or have access to all the key players around the world and in the U.S. government involved in the effort, and can help with getting the pilot up and running. With tens of thousands of manufacturers in SE Michigan, having Michigan as the pilot site nationally, this would create a lot of quality jobs and the increased movement of exports from Michigan.

To learn more about the UN\CEFACT designed standard for Single Windows for Trade Facilitation, see: http://en.wikipedia.org/wiki/Single_window

The text of President Obama’s Executive Order to establish the U.S. Single Window is available here: http://www.whitehouse.gov/the-press-office/2014/02/19/fact-sheet-president-obama-sign-executive-order-streamlining-exportimpor

Due to the need to secure supply chain invoice data from competitors, it is critically important that a Single Window encrypts all data at motion and at rest and adopts a data-centric approach to encryption that enables access to data based on role, authority, authentication status and need to know. Because supply chain payment data such as the X12 data exchanged today frequently gives away competitive intelligence, the Single Window would require a new payment system.
that can handle XML enabled encrypted contextual data in a highly secure environment. The PayThat Payment System and IAF are a perfect fit to provide value added services to a Single Window.

Because DHS, the lead agency for the U.S. Government implementation of the Single Window, must coordinate with 33 different U.S. Government Agencies which have disparate IT systems that do not readily communicate with each other, a “network of networks” architectural approach is the appropriate method to facilitate interoperability at the lowest cost while meeting the need of the Single Window to operate at the highest level of cyber security. The Single Window is of critical importance to the Department of Defense since it’s logistics arm would be one of the highest users of the Single Window services.

Benefits to Corporations that Currently Do Not Export or Import:
- Greatly simplified means to import or export via a one-stop shop for everything required
- Expert consulting services available to assist first time users
- New source of sales in global economy

Benefits to Corporations that Export or Import (and the DoD):
- Take time and cost out of transportation and manufacturing
- Eliminate blind spots in international export operations
- Many tasks will be done by e-services behind the scenes
- "Do-it-yourself" evolves into "do-it-for-me"
- Virtually co-locate shippers, railroads, truck lines, warehouse operators, and other logistics parties in a large (virtual) multi-modal transportation hub
- Get ahead of the crowd on the path to pervasive computing
- Decrease risk of terrorism inherent in the current system by orders of magnitude by giving visibility regarding who is doing what, when, well in advance for the benefit of the intelligence community’s early warning system
- Decrease insurance costs flowing from the higher security and lower risk of theft, smuggling and terrorism

Benefits to Depository Institutions and PayThat Clearing Banks
- New source of fee income value added services including:
  o Letters of credit
  o Foreign Exchange
  o Identity Management
- More rapid domestic job growth & economic growth
- Increased loan demand, especially backed by accounts receivable
- Lower risk for accounts receivable backed by e-invoices validated by the Single Window
- Increased deposits
• PayThat Clearing Banks and Depository Institutions will earn float income on all blocked good funds deposits held by the PayThat Clearing Banks
• PayThat Clearing Banks and Depository Institutions will earn fee income for all payment services that carry contextual data
• PayThat Clearing Banks and Depository Institutions will earn fee income for all value added services

The benefits for PayThat
• PayThat will earn a royalty on float income and fee income for all payment services and all value added services

The benefits for technology providers
• Vendors will be paid fees for services provided in building and assisting day to day operations of the Single Window, PayThat’s IAF, The PayThat Payment System and the PayThat Clearing Banks

Financial Model

Since the U.S. Government has funded and is building the Single Window, the cost of what is being proposed here is for building edge servers, mapping, and XML tagging data to enable interoperability. While a detailed budget has not yet been built, the cost is likely to be comparable to the healthcare model for a “network of networks” to facilitate a supply chain e-invoicing solution and financial services for exporters, in the range of $15 + to $20 million. The cost of building PayThat and the PayThat IAF is detailed elsewhere and is not included in the costs listed here.

About The Author’s Involvement in UN/CEFACT’s Single Window Standard

At the request of the U.S. Federal Reserve Bank's e-commerce office, I served as the U.S. representative from the banking industry on the UN/CEFACT committee from April 2003. South Korea, Italy and Australia and over 30 other countries are already up and running with Single Windows for trade facilitation. I have collaborated at UN/CEFACT with many of the key individuals involved in these efforts for the past decade. Prior to joining UN/CEFACT, in the 1990s I was a member of a team that led the effort to build an early version of a Single Window in the U.S. that was to be based in Detroit called the Electronic Port. Although many major collaborative partners agreed to join and support the effort, it was not funded and never was launched. These experiences could be brought to bear to assist in the creation of a successful U.S. Single Window and I would like to see it be based in Michigan.
Targeted Use Case #4: Using the Identity Assurance Federation as a Catalyst for a Depository Institution owned Credit Bureau and for a B2B Directory

Problem Statement

In the classic New Yorker cartoon, one dog says to the other, "On the Internet, nobody knows you're a dog." Until we solve this problem and know without doubt with whom we are transacting, web services cannot be made secure for internet sourced electronic payments. The U.S. payment systems used today were not architected with security built into them to do what we are doing today by extending them to payments generated from the internet. The New Yorker cartoon is from 1994, so this problem has been building for over 20 years.

"On the Internet, nobody knows you're a dog." [Please delete the cartoon before the final report is released to the public. I bought a personal license to use it from The New Yorker.- FYI]

There is no trustworthy web service that can strongly enroll and authenticate to NIST Level 3 or 4 consumers or business employees to enable sufficiently strong cyber security to safely engage in e-commerce.

To comply with Anti-Money Laundering (AML), Bank Secrecy Act (BSA) and the new Foreign Account Tax Compliance Act (FATCA) laws, each bank is now required to know and identify their customers, understand the business of each customer and understand the transactions flowing through their customers deposit accounts to non-customers. To actually and fully comply with these requirements is a near impossibility if the regulations are strictly applied, however, non-compliance carries with it the possibility of massive multi-billion dollar fines and severe reputation risk. The cost for each bank to individually do this work is far more costly and
carries much greater compliance risk than if the work were outsourced to an industry back office utility, a bank owned Identity Assurance Federation (IAF).

**Elevator Pitch**

To meet the needs to strongly enroll participants and End-Users of the PayThat Payment System and to authenticate them at NIST Level 3 or 4 on an ongoing basis, the IAF will provide a service to validate identities and perform identity management. The IAF can provide these services at much lower cost than any Depository Institution or any other party. Because the IAF builds a database of attributes related to individual and corporate participants and End-Users, the IAF can append additional data about these participants and End-Users at low cost. The appended data can be used to build a Depository Institution owned Credit Bureau and a Depository Institution owned B2B Directory. The value of the U.S. credit bureau industry, currently owned by non-banks, is $17 billion. Because much of the valuable data resident in the existing credit bureaus is supplied to them for free, the IAF’s credit bureau should be able to achieve a 60% market share of the U.S. credit bureau industry, creating $10.2 billion in value for the owners of the IAF. The B2B Directory will lower the costs of Depository Institutions by raising the amount of electronic transactions and reducing the amount of high cost paper checks.

**Description of Business Opportunity & Implementation Plan**

Businesses need access to reliable data to properly format and transact electronic payments to their customers. Banks maintain this data in disparate sources, but businesses would find it much more useful to have one secure location to obtain all the data they need and are authorized to know to initiate electronic payments.

The IAF’s identity bureau would perform the following work for all member banks:

1. Vetting the identity of each customer and the officers and shareholders of each corporate customer;
2. Understanding and vetting the business of each customer;
3. Understanding the transactions flowing through their customers deposit accounts to third-party non-customers;
4. Make recommendations for filing Suspicious Activity Reports to member banks;
5. Provide all data required to comply with local laws including FATCA reporting.
6. Provide all data required for businesses to securely access reliable data to properly format and transact electronic payments to their customers, both business customers and consumers.

The credit bureau would be able to perform these tasks at far lesser cost than individual banks can do so because of the centralization of the data and work. Under the current system each bank must perform this work for each customer. In the proposed business model, each customer and each transaction would only need to be vetted and validated as suspicious or non-suspicious.
once. The identity data on each customer and customer related party would only need to be validated once. Each transaction would only need to be vetted once and not two or more times by payer and payee banks and any intermediary banks.

The identity bureau would be able to perform these tasks far more effectively than individual banks can do so because it would have a global view of all transaction flow. Unless 100% of all global transaction activity occurs within one single bank it is impossible to meet to the letter all statutory requirements of the AML and BSA laws. However most banks have little insight into the business activities of non-customers who are the payees of customer driven transactions and therefore it is difficult if not impossible to know whether or not a given transaction is suspicious or not except at great expense. Because the identity bureau would know and have insight into ALL bank customers it could build a global view of all global transaction activity, including all payers and payees.

A searchable database of valid and authenticated electronic payment delivery instructions for every business and consumer in the U.S. would be expensive for any individual bank to provide and maintain up to date, but the identity bureau could provide secure access to this data to authorized corporate users on a need to know and secure basis. However, such a database would be created as a by-product of the required Know Your Customer, BSA, AML and FATCA compliance work.

**Key Features of a Identity Bureau**

The identity bureau would:

1. Be opt-in by both banks and bank customers. Financial incentives and disincentives would be provided to bank customers to Opt-In.
2. Optionally, banks could provide an initial level of data population to the credit bureau that was not visible to consumers aggregating all Know Your Customer, AML, BSA or FATCA data in possession of or accessible to their BSA Officers. This data could be leveraged to partially or fully automate and accelerate the Opt-In process for individual deposit account holders who are strongly authenticated.
3. Be federated using the “network of networks” architecture approach and available upon demand for a valid query, so that data is owned by individual banks and not centralized and appropriate access rules controlling each authenticated and authorized user, based on role and authority, are followed and enforced.
4. Maintain and secure an index of where relevant data resides. Each bank would select data that they are comfortable sharing and push this data on an ongoing basis to an edge server where the data would be XML tagged so the data can be easily indexed, queried and shared as appropriate.
5. Leverage the United States Postal Inspection Service (USPIS), which is the law enforcement arm of the United States Postal Service (USPS), to criminalize the act of
providing incorrect or erroneous information to the credit bureau. Unlike other law enforcement agencies in the U.S., the USPIS has a zero dollar no tolerance policy and investigates each violation referred to it. The credit bureau can leverage the USPIS at a moderate cost by using the .post top level domain of the USPS as part of its enrollment and information architecture.

6. Over time, expand the range of products and services that it's enhanced identity proofed data enables. For example:
   - Member Depository Institutions can populate credit bureau data, overdraft data and deposit account transaction flow data to gain greater insight into money flows and credit-worthiness.
   - Using transaction and enhanced contextual data flowing through the PayThat Payment System, aggregating the data from all Member Depository Institutions the IAF could create real-time business general ledgers and financial statements as a value added service. Being based on authenticated payment transactions, these financial statements would reduce the opportunity for corporate fraud. This will also reduce loan losses of member banks and gain greater insights into the credit worthiness of corporate borrowers than what can be provided by Dun & Bradstreet.

7. Provide a secure, searchable database of valid and authenticated electronic payment delivery instructions for every business and consumer in the U.S. accessible to authenticated and authorized business customers. Individual banks would designate which bank business customers are authorized and to what degree they would have access to the data.

**Value Proposition for each class of entity:**

**The benefits for processors (Depository Institutions & PayThat Clearing Banks):**
The following business drivers would motivate banks and bank customers to opt in to the proposed service:
1. As discussed above, banks which opt into this service should be able to achieve materially lower Know Your Customer, BSA, AML and FATCA compliance costs, than non-participating banks and outsource to the credit bureau a material amount of this compliance and non-compliance risk;
2. Focusing initially on customers who are active in sending international wires, banks could provide two-tier pricing to both correspondent banks and to bank customers on each end of a wire transaction.
3. Less expensive wires: Validated Opt-In Payer, Validated Opt-In Payee
4. More expensive wires: Non-Validated Payer, Non-Validated Payee

**The benefits for Participants & End-Users:**
Over time this two tier pricing model for international wires could be expanded to domestic wires and each other electronic and paper based payment type, ultimately including all
transactions and transaction accounts. Because of the reduced compliance burden on individual banks, costs truly would be lower for banks and their customers who opt-in to such a system and the current payment system would be transformed into a multi-tier pricing model, based on risk and cost.

Customers would be informed of the two tier pricing model at the time an international transaction is ordered and given an option to sign up and opt-in on the spot in real-time. Customers would also be encouraged to get non-registered payees to sign up to achieve fully discounted pricing.

Enrollment for customers at participating banks could optionally be facilitated and expedited by leveraging existing log in credentials used by customers at their Internet banking websites. Several of the future business opportunities that could be catalyzed by a successful Identity Assurance Federation offer excellent benefits to Participants & End-Users.

The benefits for PayThat:
Future business opportunities that could be catalyzed by a successful Identity Assurance Federation include:
1. Traditional Credit Bureau services - this is an opportunity to create a business with a value of at least $10 billion for the banking industry;
2. Single sign-on enhanced privacy across the web;
3. Healthcare and other non automated billing automation;
4. Elimination of Email Spam including associated costs and the massive productivity losses;
5. More secure internet-based access to bank data including transaction data;
6. Eliminate the need for PCI compliance.

Use Case Examples
Corporate Treasury User: Treasury Employee X (“X”) requires the electronic payment instructions for a new vendor. X has been authorized and authenticated by their primary bank to access the Identity Assurance Federation’s index of electronic payment delivery instructions for every business and consumer in the U.S. X logs in to the secure site and initiates a query using the search function of the secure site using the information in her possession about the business. Valid payment instructions are retrieved and automatically imported into her firm’s accounts payable automation software. An ACH transaction is initiated automatically on the payment due date by the accounts payable automation software.

The next payee that X requires information on, is a consumer who is due a $20 refund on a purchase return or billing correction adjustment. Instead of formatting and mailing a check, X logs in to the secure site and initiates a query using the search function of the secure site using the information in her possession about the consumer. Valid payment instructions are retrieved
and automatically imported into her firm’s accounts payable automation software. An ACH transaction is initiated automatically on the payment due date by the accounts payable automation software.

**Bank Employee User:** Bank BSA Officer Z (“Z”) has received an electronic message informing her that a pending transaction is deemed suspicious by the Identity Assurance Federation’s KYC/BSA/AML identity management department. Z logs in to the secure site and reviews the secure message and the attached research findings indicating why the pending transaction is deemed suspicious. The recommendation is to allow the transaction to proceed but to file an SAR. A draft of the proposed SAR including all required fields pre-populated is available for review by Z. Z reviews the data provided and the draft SAR and concurs with the recommendations. The SAR is automatically filed and a copy of all supporting data is archived for future secure retrieval.

USA PATRIOT Act Section 314(b) permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. Bank Y has opted in to Section 314(b). Employee Z receives a Section 314(b) request via a secure electronic message from Identity Assurance Federation’s KYC/BSA/AML identity management department. Z logs in to the secure site and reviews the secure message and the attached request. Z authorizes the release of all data regarding that customer and access to that data is provided securely to the requesting bank.

Bank Officer Q is responsible for ensuring FATCA compliance for their deposit account holders. To ensure all U.S. related accounts are properly identified, including beneficial owners, Bank Officer Q subscribes to the Identity Assurance Federation’s FATCA service. Q logs in to the secure site and uploads a data file with the requested information on its deposit holders. Q receives back a report identifying all U.S. account holders and details of how and what is known that indicates the account is related to a U.S. person or entity. Without further work, Q receives future automated updates if the status of any of the bank’s deposit holders changes and it becomes a U.S. related account or ceases to be a U.S. related account.

**Next Steps - Piloting an Identity Bureau**

To launch a identity bureau, the following participants are required:

1. Initial bank participants, including at least two of the four U.S. mega banks, since that would provide required critical mass, and at least one community bank, to validate that the service can be cost efficient and affordable for banks of all sizes (University Bank is willing to serve in that role);

2. A system integrator familiar with building and deploying SOA cloud based services such as CNSI, which built a system using similar IT infrastructure principles as what is proposed

3. A secure Internet hosting service provider, such as CSC, which hosts highly secure facilities of this type for the U.S. government.

4. Official representatives of government bank regulators involved in KYC/AML/BSA/FATCA compliance, such as the Federal Reserve, U.S. Treasury FINCEN and CFPB.

5. SWIFT and/or The Clearing House and/or the Fed's International ACH team, since international transactions would be the initial pilot focus.

Pilot program participants would determine the specific next steps and pilot program deliverables, but at a minimum the pilot would include the following:

1. A SOA/cloud based data sharing service, including:
   a. An index of available data;
   b. Ability to query on demand;
   c. An enrollment mechanism;
   d. A data dictionary standard for XML data to be shared among the credit bureau members using an international standard such as an ISO or UN CEFACT standard.
   e. A reference implementation of the edge data server each participating bank would create to share data with participating banks;
   f. A data sharing and use agreement binding the participating banks;
   g. Reference data mapping implementations demonstrating the ability to translate bidirectionally the data on a bank's edge server into or from the data dictionary standard without loss of data.

2. The credit bureau would improve the quality of the KYC/AML/BSA/FATCA work being performed by participating banks while reducing the KYC/AML/BSA/FATCA workload on each individual bank.

3. Validation by banking regulators that banks that use the credit bureau service will receive preferential treatment in resolving compliance issues related to KYC/AML/BSA/FATCA compliance for electronic transactions.

Financial Model
The cost of the IAF is included in the quoted figure for Use Case #2, see above.

The benefits for technology providers
Vendors will be paid fees for services provided in building and assisting day to day operations of SEMHIE, PayThat’s IAF, The PayThat Payment System and the PayThat Clearing Banks Timing for pilot implementation is up to the pilot participants, however, this should readily be achievable in less than 18 months since University Bank and the vendor team mentioned above completed a program to create an entire health history for individuals using a similar architecture in that same amount of time. An individual's health history involves much more complicated
data than anything contemplated here. The ICD-10 healthcare code set allows more than 14,400 different codes.

3. Integration Effort

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

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

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

Because PayThat uses a “network of networks” architectural approach leveraging:

- XML
- XML tagged data pushed to edge servers from legacy applications
- Mapping; and
- Interoperability standards

interoperability among legacy infrastructures such as legacy bank platforms and bank payment systems can be ensured, extending their usefulness and dramatically lowering cost of adoption for innovative solutions. The points of integration are greatly reduced and legacy systems are unaffected in their daily operation.

In the PayThat use cases, the only points of integration are between the PayThat Clearing Banks, which serve as “edge servers” for traditional Depository Institutions and the payment systems of those traditional Depository Institutions. The integration required is equivalent to a banking corporate treasury workstation. The integration is modest and should only take weeks. By design and purposefully the amount of IT integration with the systems of legacy Depository Institutions is kept to a minimal level. Since most corporate treasury workstation solutions support data exporting and data importing, the challenge is mostly reduced to mapping and by using state of the art mapping automation tools, which have low six figure costs, the technical challenge is low and the technical risk is low. The only point at which there is a point of
introduction in the eight stages of the payment lifecycle (as discussed in Part A) is when good funds are to be loaded into PayThat or taken out of PayThat. This is as simple as a credit or debit message using the corporate treasury workstation between the traditional Depository Institution and the PayThat Clearing Bank. All the other functions occur within the new PayThat Payment System network, and are described elsewhere in detail.

Creating XML tagged databases is also a task where the technical challenge is low and the technical risk is low. Where any of the use cases require interaction with any pre-existing legacy solution, the same architectural approach and means of integrating and creating a means of enabling data interoperability will be used: data will be pushed to edge servers from legacy applications, where the data is XML tagged by individual data element and encrypted with Persistent Digital Security. This applies to non-bank account provider (for origination and receipt on behalf of end users), third-party service providers, merchants (e.g., PoS and eCommerce), billers, consumers and businesses. The “edge server” for consumers and businesses is the CashBox, already described in detail above, as well as how it integrates with other existing software systems and hardware devices. For merchants, billers, third-party service providers and non-bank account providers, they will need to install “edge servers” in their existing operations, to interoperate data between their existing systems and the PayThat Payment System. For each vendor solution, whether it is software or a device, the vendor will be incentivized to create the mapping and since PayThat will provide published APIs using open standards for these interfaces, the cost and complexity of the job will be relatively easy, a matter of weeks of programming to modify existing systems.

By using a “Data-Centric” approach to encryption where data access is controlled by role & authority on a transaction level basis, access to all data is controlled by users at the network nodes where the edge servers reside with access controlled by rules enforced by strong encryption, providing greater control & security. Legacy systems that do not have the ability to conform to the data-centric approach can still be used in production, as interoperability can be achieved via the edge servers, with data flowing in both directions. When data is inside the corporate network it can be locked down so that it is not exposed to the internet and existing data controls apply even if it is not encrypted in motion or at rest. When data is pushed to edge servers from legacy applications, it is immediately XML tagged and encrypted with Persistent Digital Security.

As noted above, the Author was part of a team that built the first Health Information Exchange in the U.S. using the “network of networks” architecture approach that has now been designated a best practice by the HHS Office of the National Coordinator for Health Information Technology. It is illustrative to explore in depth the example of the systems built that he has been closely involved in to understand the efficiencies that are gained and what types of systems this architectural approach works best.
Some healthcare professionals argued that a single large database and single vendor solution could succeed in providing efficient Health Information Exchange. The HIE “single network/single solution/single database” (SSS) concept works well in small and moderate size communities where there is one dominant provider of healthcare services who can dictate that one solution be adopted by the entire medical trading area. In communities where there is not one dominant provider, where the HIE “SSS” concept has been tried, such as Long Beach (CA), Boston (MA) and New York State, hundreds of millions of dollars in each community were spent and lost on deploying the HIE “SSS” concept and the projects failed because interoperability could not be achieved. The health systems did not embrace these HIEs in their daily operations and those projects failed because the HIE “SSS” prevented them from seamlessly using their existing legacy solutions in which each health system had invested hundreds of millions of dollars.

The Detroit area health system CIOs thoroughly explored this HIE “SSS” option with Covisint and rejected it as not meeting the needs of their health systems. Similar HIE “SSS” based solutions were also rejected. A thorough assessment process was conducted by CIOs of the local major health systems. This is why SEMHIE moved towards a “network of network” architectural approach.

In Michigan Spectrum Health in Grand Rapids adopted Medicity and Sparrow Hospital in Lansing adopted Axolotl. They decided to go with the HIE “SSS” route because each health system dominates their medical trading area. However their CIOs (and a very large group of statewide health IT experts) endorsed the “MHA Sub-state HIE Interoperability Strategy & Architecture” which incorporates a “network of network” architecture identical to SEMHIE’s to provide the interoperability statewide and nationally of the state’s HIEs including SEMHIE’s, Spectrum Health’s and Sparrow Hospital’s HIEs.

SEMHIE built and is now live in production generating and transmitting CCDs from Henry Ford Health System and Oakwood Health System to the Social Security Administration across its HIE network. The build-out, testing and vetting process was completed for under $1.3 million, less than two orders of magnitude lower than the failed NY, Boston and LA projects.

CSC and CNSI, who are major health IT vendors, built the SEMHIE system on the basis that they will not be paid unless it works. These firms were 2 of the 4 major nationwide technology companies who built the National Health Information Exchange. This decision was made at the highest levels of those firms because they know, if they can solve the problem here in Michigan, they can go back to Los Angeles, Boston and New York State and “fix” those HIEs and make money doing so.

If a health system adopts the HIE “SSS” architecture instead of SEMHIE’s “network of network” system (also now adopted as the statewide interoperability architecture), they risk spending hundreds of millions of dollars instead of a few million on an IT methodology that has failed
repeatedly in complex medical trading areas where there is not one dominant provider of healthcare services.

We have proven conclusively that the “network of network” system approach works, and the HIE “SSS” IT design fails in complex healthcare medical trading areas like Detroit.

Creating interoperability in the U.S. banking industry where there is no one dominant provider while continuing to use the legacy systems where tens of billions of dollars of sunk costs are invested poses very similar challenges to those faced by the healthcare industry and the health information exchange industry.

While the “network of networks” architectural approach is now proven as lower in cost by orders of magnitude and capable of solving interoperability challenges in highly complex systems with multiple entities, none of whom has the market power to dictate a one size fits all solution, there are some issues related to integration that are not yet proven in the “network of networks” architectural approach.

Encryption key management protocols do not interoperate across networks and different vendor identity management solutions do not interoperate across networks. The whole goal of NSTIC is to develop a common business model for key management and digital credential vendor solutions to interoperate. OASIS does have a Key Management Integration Protocol Standard. We believe that an implementation of this standard can solve both issues. Some NSTIC pilots have started to prove this, however the Author has not been directly involved in any of those pilots and while the Author firmly believes that these solutions will be proven, he does not yet have proof that these solutions do actually scale at reasonable cost with hundreds of millions of End-Users and Participants. Any other approach however, will be 10 to 100 times more expensive and much more likely to fail, short of a government mandate to force one and only one solution on the market for a single encryption key management protocol. To do this would require the government to mandate the use of one and only one encryption vendor’s solution to the exclusion of all others, which would introduce greater chance of catastrophic failure if there was a cyber breach.
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

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

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

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

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

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

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

[Please note some page numbers in the following tables under the “Reference” column may have shifted slightly by a page forward or back due to final edits of the document. Please look one page forward or back if the material suggested has moved.]

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
</tbody>
</table>
| Ubiquity | U.2 | Usability | X | 1: 10, 15, 27, 84, 97  
2: 10, 15, 42, 47, 52, 85, 15, 24-27, 29  
3: 34, 41, 44, 95, 27-30, 34-36, 38-40, 43  
4: 27 |
|----------|-----|-----------|---|-------------------------|
| Ubiquity | U.3 | Predictability | X | 1: 69, 70, 118  
2: 48, 50, 54, 58, 62, 65, 37, 38, 41, 42, 46, 47, 70  
3: 9-10, 14-15, 24, 26, 28-29, 33-36, 42, 44, 48, 52, 76  
4: 69, 70, 118  
5: 37, 38, 41, 42, 46, 47, 70  
6: 10, 21 |
| Ubiquity | U.4 | Contextual data capability | X | 1 & 2: 39, 40, 49, 50  
3: 49 |
2: 20-21, 49, 51-54, 116  
3: 54, 58, |
## Justification for U.1:

*Discuss self-assessment addressing considerations U.1.1 to U.1.6*

U.1.1: Through its integration with legacy bank payment systems, PayThat can load value from any type of account at any Depository Institution in the United States. All Regulated Non-Bank Account Providers carry their accounts at one or more Depository Institution and their accounts can be accessed via ACH and Wire, if not other electronic payment methods. Similarly, PayThat can load value to any type of account at any Depository Institution in the United States.

U.1.2: Through its ability to send payments to any email address or mobile phone enabled with SMS (text message) capability and the fact that virtually everyone in the U.S. including the unbanked have nearly universal access to email or mobile phone texting, PayThat can reach nearly the entire population of the U.S.

U.1.3: Through the CashBox, PayThat Tokens and Global Payment Gateway, PayThat supports multi-currency payments.

U.1.4: Through its ability to send payments to any email address or mobile phone enabled with SMS (text message) capability and the fact that virtually everyone in the U.S. including the unbanked have nearly universal access to email or mobile phone texting, PayThat can reach nearly the entire population of the U.S. An entire proposal supporting unbanked marketing and deployment is available under MNDA.

U.1.5: PayThat has provided four detailed use cases supporting a credible plan for achieving widespread adoption. Using the “network of networks” architectural solution and “edge servers”, PayThat is technically feasible at reasonable cost for Providers of all types to adopt without needing to spend large amounts of funds to integrate with existing legacy solutions. The value proposition for Providers to make PayThat available to End-Users is laid out in the four use cases.

U.1.6: Using the “network of networks” architectural solution and “edge servers”, PayThat is able to integrate with existing legacy solutions across networks and multiple operators. The PayThat message flow and eight payment messages demonstrate how a payment initiated by one Provider (FI-1) can be received by a User (S-2) server by another Provider (FI-2)
Justification for U.2:  
[Discuss self-assessment addressing considerations U.2.1 to U.2.4]  
U.2.1: PayThat is device, channel and platform agnostic. SMTP and SMS protocols are easily interoperable with any circumstance.  
U.2.2: PayThat requires only an email address or mobile phone enabled with SMS (text message) capability to send a payment. Regardless of the transmission method, the receiver (S-2) must be strongly enrolled and strongly authenticated. To open the .pay file and access its contents including the money contained in it, S-2 must be an enrolled PayThat participant and authenticate themselves to the IAF (the Authentication Server) or log in to their Depository Institution’s participants existing online banking or mobile banking services.  
U.2.3: PayThat is accessible to End-Users on a 24x7x365 basis for payment initiation, pending transaction status and receipts, and for availability of good funds. Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages, being all automated, should take under two seconds. For use cases where Sigma 5 or Sigma 6 reliability is required, more expensive and reliable networks with guaranteed uptime can be used to communicate among the parties involved in a transaction.  
U.2.4: Because the PayThat Payment System is device agnostic provided that the device is reasonably secure, vision or hearing impaired individuals, individuals with other disabilities, the elderly and individuals with limited English proficiency will be able to use their existing devices and assistive methods that they use currently to access internet, cell phone or web services, ensuring widespread usability. In addition, the CashBox utilizes a GUI menu that is very simple with few options, however by turning on additional optional services and menu options, a user can access higher levels of complexity in using PayThat, if desired. Participants will therefore have the ability to use PayThat at the level of technological proficiency that they themselves desire.

Justification for U.3:  
[Discuss self-assessment addressing considerations U.3.1 to U.3.6]  
U.3.1: The core features of PayThat: the CashBox, PayThat Clearing Banks, eight messages, four databases and the IAF’s enrollment and authentication services, are uniform across the PayThat Payment System by design. The same components are used by all Parties.  
U.3.2: The PayThat Payment System rules apply to all End-Users and are in compliance with Regulations E and Z, as applicable. Consumers themselves control many aspects of the data privacy of their data resident in the PayThat system by selecting among three levels of privacy controls. All fees are fully disclosed prior to incurring the fees and what each use cases and optional value added service does and what it cost are explained by the CashBox prior to an End-User committing to it.  
U.3.3: PayThat’s messaging uses email (SMTP) and text messaging (SMS) standards for all communication.
U.3.4: The core features of PayThat: the CashBox, PayThat Clearing Banks, eight messages, four databases and the IAF’s enrollment and authentication services, are uniform across the PayThat Payment System by design. The same components are used by all Parties.

U.3.5: PayThat’s error resolution process follows Regulation E and Regulation Z.

U.3.6: PayThat is a good intuitive natural speech based brand. When one is asked if they want to buy something for a certain price they say in reply please Pay That amount. The PayThat.com and PayThat.net domains are available for use with this brand.

**Justification for U.4:**

[Discuss self-assessment addressing considerations U.4.1 to U.4.3]

U.4.1 & 4.2: PayThat supports rich, XML interoperable contextual data, as well as open APIs and help wizards to assist with interoperability and integration. The open API and help wizard automate the process of pulling data into standard industry business and personal finance systems (e.g. accounts payable, accounts receivable, claims processing, payroll, treasury workstation, ERP systems, Consumer accounting software and tax reporting software). At a minimum, even if a specific API isn’t available for a system, the open API data can as a default be exported using comma delimited excel files, since excel is the most common software used to support business data interchange. The open API also enables vendors to provide an ecosystem of value added services. PayThat also supports STP820 messaging, ISO20022 messages, X12 data and UN CEFACT XML data.

U.4.3: PayThat supports all the key industry standards for contextual payment data: STP820 messaging, ISO20022 messages, X12 data and UN CEFACT XML data. The PayThat CashBox open API data can as a default be exported using comma delimited excel files, since excel is the most common software used to support business data interchange.

**Justification for U.5:**

[Discuss self-assessment addressing considerations U.5.1 to U.5.5]

U.5.1: The CashBox provides easy and immediate access to convenient, cost effective and rapid cross-border payments and the Global Payment Gateway provides easy interoperability with overseas payment systems, based on the “network of networks” architectural design.

U.5.2: PayThat uses ISO20022 and UN CEFACT XML standards to support interoperability.

U.5.3: PayThat requires that all fees, rates and terms are disclosed to the participant (S-1 & S-2) prior to initiating a transaction.

U.5.4: PayThat supports real-time multi-currency conversion. PayThat Tokens may be denominated in any currency.

U.5.5: PayThat supports real-time multi-currency conversion. The Global Payment Gateway implementation plan outlines the timelines anticipated.

**Justification for U.6:**

[Discuss self-assessment]

PayThat supports each of the use cases targeted by the Federal Reserve. Four specific business plans are outlined in the proposal. PayThat can support any use case including...
micro-payments, macro-payments, payments with contextual data, and could serve as a more secure replacement for any of the existing legacy electronic payment systems.

2. **Efficiency**

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

**Self-assessed rating:**

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

**Justification for E.1:**
[Discuss self-assessment addressing considerations E.1.1 to E.1.4]
E.1.1 & 1.2: End-Users may opt to use one, two or more PayThat Clearing Banks and may freely change with whom they do business.
E.1.3: During the initial enrollment process PayThat Clearing Banks are required to fully disclose all fees, terms and conditions applicable to their PayThat account.
E.1.4: The PayThat Payment System allows banks of all sizes to provide services on an equal access basis provided that the bank can meet the PayThat Payment System rules applicable to all banks.

**Justification for E.2:**
[Discuss self-assessment addressing considerations E.2.1 to E.2.3]
E.2.1 PayThat supports rich, XML interoperable contextual data, as well as open published APIs and help wizards to assist with interoperability and integration.
E.2.2 PayThat’s open API for exporting data and the ability to import contextual data also through an open API enables vendors of any type to provide an ecosystem of value added services.
E.2.3 Any of these value added services would be required under the PayThat Payment System rules to fully disclose to any End-User opting to use these services any fees for these additional optional services and that these services are optional, prior to incurring any fees.

**Justification for E.3:**
[Discuss self-assessment addressing consideration E.3.1]
E.3: PayThat achieves initial implementation within 18 months of launch and ubiquity prior to 2020.
E.3.1: The chosen initial use cases are designed to achieve 40% market share of the market segment within 18 months following launch. This assures that PayThat will always have the number one market share in its chosen segments and will never be relegated to the number two market share position. The chosen use cases are designed to be attractive to risk capital sourced from both Depository Institutions and venture capital firms, based on the prospective returns and value created.

Justification for E.4:
[Discuss self-assessment addressing considerations E.4.1 to E.4.5]
PayThat supports all the key industry standards for contextual payment data: STP820 messaging, ISO20022 messages, X12 data and UN CEFACT XML data. The PayThat CashBox open API data can as a default be exported using comma delimited excel files, since excel is the most common software used to support business data interchange. The are widely used, cost effective (E.4.3), standards based (E.4.5), interoperable (E.4.1) and widely deployed globally (E.4.2). PayThat supports open APIs and its XML enabled databases would support any future innovative payment format standards (E.4.4).

Justification for E.5:
[Discuss self-assessment addressing considerations E.5.1 to E.5.2]
E.5.1: PayThat supports all eight stages of the end-to-end payments process.
E.5.2: The technical design of PayThat comprehensively supports all proposed features including usability [easy to use as email and texts], reliability [Sigma 4-6 as needed, see pages 35, 37, 38, 40, 44], performance [the eight messages provide redundancy to ensure integrity of the messaging process, see pages 27-49], information security protocols [extensively discussed throughout the document], operations [ditto], compliance controls [see discussion of audits on pages 48,73, 85, 98], and risk controls [see discussion of risk on pages 12, 25, 31, 32, 42, 43, 44, 48].

Justification for E.6:
[Discuss self-assessment addressing considerations E.6.1 to E.6.3]
E. 6.1: The “network of networks” architecture is proven and capable of processing high volumes of XML data.
E. 6.2: SWIFTNet runs a XML compatible payment system with high transaction volumes without difficulty at comparable transaction levels to what VISANet handles. The technical design capacity was validated by the former CTO of Daimler Chrysler at much higher velocity.
E. 6.3: The “network of networks” architecture is extremely adaptable and flexible as it can interoperate with any legacy system able to push data to an edge server.

Justification for E.7:
[Discuss self-assessment addressing considerations E.7.1 to E.7.3]
E.7.1: Management of Identity Enrollment exceptions are discussed on pages 26 and 80, the Regulation E error resolution process is discussed on pages 42, 47 and 70, CashBox complaint resolution is discussed on pages 47 and 70, Management of GPG exceptions are discussed on page 52, healthcare payments on page 77. The ability of the PayThat Clearing Banks to block funds and block transactions that are deemed suspicious is discussed on pages 37, 39, 41, 46.

E.7.2: Information is stored in four PayThat databases: CIF & Pending Transactions (see page 29), Authentication Server (see page 32) and Cleared Transactions (see pages 42 and 45) and the network diagram on page 28. Retention is discussed on page 47, audit on pages 48, 73, 85, 98.

E.7.3: Network monitoring is discussed on page 47.

3. Safety and Security

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

### Self-assessed rating:

<table>
<thead>
<tr>
<th>Criteria Name</th>
<th>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>X</td>
<td>48</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.2 Payer authorization</td>
<td>X</td>
<td>1: 33-35, 24-33, 2 &amp; 3: 34</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.4 Settlement approach</td>
<td>X</td>
<td>1: 43-44, 2: 44, 3: 43-44</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.5 Handling disputed payments</td>
<td>X</td>
<td>1: 37, 41, 46, 71, 33, 34</td>
</tr>
<tr>
<td>Effectiveness Criteria</td>
<td>Effectiveness Criteria Self-Assessment (Check One)</td>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Criteria Name</td>
<td>Consideration Name</td>
<td>VE</td>
<td>E</td>
</tr>
</tbody>
</table>
| Safety and Security    | S.6              | X |    |    |    | 1: 47-48  
|                        |                  |    |    |    |    | 2: 71, 47-48  
|                        |                  |    |    |    |    | 3: 47-48  
|                        |                  |    |    |    |    | 4: 10  
|                        |                  |    |    |    |    | 5: 29, 32, 42, 45, 28  
|                        |                  |    |    |    |    | 6: 28  
|                        |                  |    |    |    |    | 7: 48  
|                        |                  |    |    |    |    | 2: 48-49  
|                        |                  |    |    |    |    | 3: 48-49  
| Safety and Security    | S.8              | X |    |    |    | 1: 49  
|                        |                  |    |    |    |    | 2-5: 48  
<p>| Safety and Security    | S.9              | X |    |    |    | 1: 32, 34, 35, 37, 39, 41, 45, 54, 108, 26, 49 |</p>
<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name # Consideration Name</td>
<td>VE E SE NE</td>
<td>Proposal Page Number</td>
</tr>
</tbody>
</table>

**Justification for S.1:**

*Discuss self-assessment addressing considerations S.1.1 to S.1.6*

A detailed statement regarding risk management covering all items (S.1.1 to S.1.6) is on pages 48-49. Sanctions are available to PayThat to expel any entity that is non-compliant with the PayThat System rules (S.1.5, see page 49). PayThat can examine Depository Institutions and PayThat Clearing Banks to determine their compliance with the rules.
Justification for S.2:
[Discuss self-assessment addressing considerations S.2.1 to S.2.3]
S.2.1: PayThat requires the Payer (S-1) to authorize each transaction prior to initiation (see Payer Authorization pages 33-35 and Initiation pages 24-33).
S.2.2 & S.2.3: Pre-authorization, pending pre-authorized transactions and revocation of pre-authorized transactions are discussed on page 34.

Justification for S.3:
[Discuss self-assessment addressing considerations S.3.1 to S.3.3]
S.3.1: Approval by the Payer’s Provider following payment initiation to ensure S-1 has good funds available, is discussed on pages 35-36.
S.3.2: Payment finality is discussed on pages 41 and 36-39. Pending transactions not yet cleared are visible once the first message arrives in S-2’s CashBox.
S.3.3: Disputed payments and Regulation E are discussed on page 41.

Justification for S.4:
[Discuss self-assessment addressing considerations S.4.1 to S.4.3]
S.4.1: Settlement including the method and periodicity of settlement, hours of operation, how settlement capability is ensured, and correspondent related settlement issues are discussed on pages 43-44.
S.4.2: Settlement related liquidity analysis and controls and 24/7/265 operations are discussed on page 44.
S.4.3: PayThat uses Central Bank money or correspondent account settlement, as discussed on pages 43 and 44.

Justification for S.5:
[Discuss self-assessment addressing considerations S.5.1 to S.5.5]
S.5.1: PayThat has the ability to block funds in accounts during investigations and to reset the funds in accounts when an error has been made (see pages 37, 41, 46). Customer complaints and fraud reports can be handled by existing bank operations and existing channels for handling Regulation E issues (see page 71). Instances of identity fraud will be referred to the U.S. Postal Inspection Service, the federal law enforcement and security arm of the U.S. Postal Service (see pages 33, 48, 71, 81, 113).
S.5.2: Customer complaints and fraud reports can be handled by existing bank operations and existing channels for handling Regulation E issues (see page 71).
S.5.3: Pending transactions and the individual receipts for each completed transaction stored in a Participant’s CashBox have a button a Participant may manually trigger that automatically reports a transaction to their PayThat Clearing Bank as fraudulent, erroneous or unauthorized (see pages 42, 46).
S.5.4: Customer complaints and fraud reports can be handled by existing bank operations and existing channels for handling Regulation E type issues (see page 71).
S.5.5: Customer complaints and fraud reports can be handled by existing bank operations and existing channels for handling Regulation E issues (see page 71).

**Justification for S.6:**

[Discuss self-assessment addressing considerations S.6.1 to S.6.7]

S.6.1: The IAF will be responsible for facilitating timely and frequent sharing of information among all Providers, operators and regulators to help them manage, monitor, and mitigate Fraud and evolving threats in accordance with applicable law. Information shared for anti-fraud activities shall be used only for fraud management purposes and this will be enforced by the encryption of the data elements shared. All data shared shall remain fully encrypted at rest and in motion, including PII, and PII shall be excluded from information sharing when possible. If shared, data shall only be accessible based on role, authority, authentication status and need to know (see pages 47-48).

S.6.2: The Identity Assurance Federation manages the four PayThat Payment System databases which are secured pursuant to ISO encryption standards and the methods taught in the patents of Jove Corporation and TecSec, so that each data element is individually accessible or not accessible, based on authenticated status, role, authority and need to know (see page 71 and see pages 47-48 for additional detail regarding the use of FFIEC standards to protect the databases and data centers).

S.6.3: The IAF will be responsible for facilitating timely and frequent sharing of information among all Providers, operators and regulators to help them manage, monitor, and mitigate Fraud and evolving threats in accordance with applicable law (see pages 47-48). The four databases including aggregated data from each step of the business process from authentication to pending transactions to cleared transactions.

S.6.4: The IAF uses email and text messages to communicate with other parties, including for fraud information sharing (see page 10).

S.6.5: CIF & Pending Transactions (see page 29), Authentication Server (see page 32) and Cleared Transactions (see pages 42 and 45) and the network diagram on page 28.

S.6.6: The IAF is the central trusted repository to store and aggregate the information in the four databases (see the network diagram on page 28).

S.6.7: The IAF is responsible for managing the fraud detection system, which includes among its goals patterns at the individual or aggregate level suggestive of risk (see page 48);

**Justification for S.7:**

[Discuss self-assessment addressing considerations S.7.1 to S.7.3]

S.7.1: PayThat has strong technical access components and controls including: IdM (see pages 24-33), data encryption at motion and at rest (pages 32, 34, 35, 37, 39, 41, 45, 54, 108), data quality and integrity is assured by means of the confirmations sent between the four parties to confirm receipt of each instruction and to validate that the contents of the encrypted files being used as receipts were not altered or tampered with following payment initiation (page 41), all nodes in the PayThat Payment System will be protected by state of the art cyber security protection, monitoring and malicious pattern detection systems that perform
and facilitate data breach prevention and detection (page 47), PayThat relies on data-centric layered security controls, where *Persistent Digital Security* encryption wrappers enhance privacy to secure payments and transaction detail. The message structure has multiple layers of encryption wrappers each with a different key required to open them to enable variable access based on role, authority, need to know and authentication status. For example, one layer implements the privacy template controls and another layer implements the extra security surrounding the PayThat Tokens (pages 9, 11, 15, 85-87, 98-99, 103, 119), various components and controls such as the IAF and the CashBox leverage many robust industry standards such as ISO20022, FFIEC Security Standards, Unified Modeling Language, ANSI X9 Encryption Standards, UN CEFACT XML, SMTP, SMS, TCP/IP, FSTC Financial Agent Secure Transaction, Kantara Initiative Identity Management framework, UN CEFACT Single Window, Trusted Platform Module, Automatic Number Identification, Asymmetric Cryptographic Key Pairs, NIST 800-63-2, UPU, IPv6, NSTIC, SAML, STP820, SOA, CCD, Health Plan Identifier, CAQH CORE, FIPS 140-2, NIST SP-800-145, NACHA CCD+Addenda, OASIS Key Management Integration Protocol, Advanced Encryption Standard, I-9 standard and ICD-10 are some of the keys one deployed in the PayThat solution.

S.7.2: The PayThat data retention policy and disposal process is summarized on page 47. The following items are addressed on pages 48-49:
- Physical security including physical access security
- Network monitoring and incident response
- Business disaster recovery and business resiliency & target availability plans and policies
- Enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process
- Internal and external audits
- An annual Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, SSAE 16
- Periodic contingency testing and mock disaster scenario drills.
- Change management including those caused by technology and regulation changes
- Internal or external fraud or errors
- Periodic review and update

S.7.3: The IAF managed four databases and each PayThat Clearing Bank will be physically housing in enterprise network server data centers compliant with FFIEC standards for vendors for Depository Institutions. The data centers will incorporate (the following list on pages 48-49 is intended only to highlight at a high level some of the many FFIEC standards) policies, procedures and rules regarding:
- Enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process
• FFIEC IT standards
• Periodic review and update

Justification for S.8:
[Discuss self-assessment addressing considerations S.8.1 to S.8.5]
S.8.1: The IAF managed four databases and each PayThat Clearing Bank will incorporate FFIEC compliant policies, procedures and rules regarding Sigma 6 uptime, by ensuring all mission critical systems have geographically separated immediate fail-over redundancy, including POPs, servers and web services (see page 49).
S.8.2: The IAF managed four databases and each PayThat Clearing Bank will incorporate FFIEC compliant policies, procedures and rules regarding business disaster recovery and business resiliency & target availability plans and policies, enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process, internal and external audits, an annual Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, SSAE 16, periodic contingency testing and mock disaster scenario drills across the PayThat Payment System (see page 48).
S.8.3: The IAF managed four databases and each PayThat Clearing Bank will incorporate FFIEC compliant policies, procedures and rules regarding (see page 48):
• Physical security including physical access security
• Network monitoring and incident response
• Business disaster recovery and business resiliency & target availability plans and policies
• Enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process
• Internal and external audits
• An annual Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, SSAE 16
• Periodic contingency testing and mock disaster scenario drills across the PayThat Payment System.
• Change management including those caused by technology and regulation changes
• Internal or external fraud or errors
  In addition, since the PayThat Payment System operates using stored value in blocked accounts, if there was a catastrophic failure, since the funds are stored outside of the system, the likelihood that the PayThat Payment System causes an event that triggers systemic risk is less likely than an event at the actual depository bank holding the funds.
S.8.4: The IAF managed four databases and each PayThat Clearing Bank will incorporate FFIEC compliant policies, procedures and rules regarding (see page 48):
• Business disaster recovery and business resiliency & target availability plans and policies
• Enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process
• Internal and external audits (which confirm that sufficient resources are being devoted to compliance with the policies, procedures and rules)
• An annual Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, SSAE 16
• Periodic contingency testing and mock disaster scenario drills across the PayThat Payment System.
• Change management including those caused by technology and regulation changes
• Internal or external fraud or errors
• Periodic review and update
To pass an FFIEC IT Audit, sufficient resources must be devoted to comply with these and other requirements ensuring business continuity and resiliency.
S.8.5: The IAF managed four databases and each PayThat Clearing Bank will incorporate FFIEC compliant policies, procedures and rules regarding (see page 48) periodic contingency testing and mock disaster scenario drills across the PayThat Payment System.

**Justification for S.9:**

*Discuss self-assessment addressing considerations S.9.1 to S.9.3*

S.9.1: PayThat requires all data in the PayThat Payment System and the four databases managed by the IAF to encrypt all data at motion and at rest (pages 32, 34, 35, 37, 39, 41, 45, 54, 108). PII will not be used to authenticate transactions once an End-User is strongly enrolled. The PayThat payment system will accumulate PII data in an encrypted database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only (see page 26). The PayThat Payment System rules will ensure that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules, including those applicable to End-Users and can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures (see page 49).

S.9.2: PayThat requires all data in the PayThat Payment System and the four databases managed by the IAF to encrypt all data at motion and at rest (pages 32, 34, 35, 37, 39, 41, 45, 54, 108). PII will not be used to authenticate transactions once an End-User is strongly enrolled. The PayThat payment system will accumulate PII data in an encrypted database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only (see page 26). Account numbers need to be known by FI-1 and FI-2 but never by S-1 or S-2, since their respective Depository Institutions know their customers via alternative means using the SSO or IAF process (see page 40).
S.9.3: Account numbers need to be known by FI-1 and FI-2 but never by S-1 or S-2, since their respective Depository Institutions know their customers via alternative means using the SSO or IAF process (see page 40). PayThat requires all data in the PayThat Payment System and the four databases managed by the IAF to encrypt all data at motion and at rest (pages 32, 34, 35, 37, 39, 41, 45, 54, 108). PII will not be used to authenticate transactions once an End-User is strongly enrolled. The PayThat payment system will accumulate PII data in an encrypted database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only (see page 26). The PayThat Payment System rules will ensure that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules, including those applicable to End-Users and can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures (see page 49).

Justification for S.10:
[Discuss self-assessment addressing considerations S.10.1 to S.10.6]
S.10.1: PayThat uses the NIST 800-63-2 standard for enrollment and ongoing authentication. The level of assurance of identity proofing will rise from Level 1 to Level 4 per the NIST 800-63-2 standard based on risk and the dollar size of a proposed transaction (page 25).
S.10.2: To deposit a payment S-2 must gain access to the CashBox on the strongly authenticated and strongly enrolled device and S-2 must be enrolled and authenticated. If S-2 cannot authenticate their identity to the IAF and/or to FI-2, they cannot open the .pay file and will not be able to deposit the funds into FI-2 or even view the contents of the .pay file or manipulate it in any way. FI-2 must validate S-2 as an authorized participant to enable S-2 to have any access to the .pay file (pages 35-36). The IAF is responsible for managing the fraud detection system, which includes among its goals patterns at the individual or aggregate level suggestive of risk (see page 48).
S.10.3: PayThat uses the NIST 800-63-2 standard for enrollment and ongoing authentication. The level of assurance of identity proofing will rise from Level 1 to Level 4 per the NIST 800-63-2 standard based on risk and the dollar size of a proposed transaction. PayThat uses two or more factor authentication including a physical trait – a biometric such as a voiceprint or fingerprint, captured during the strong enrollment process – with a personal possession, such as a smart phone, which is strongly enrolled and strongly authenticated, using the device’s Trusted Platform Module (TPM) chip and Automatic Number Identification (ANI). The TPM chip contains an Asymmetric Cryptographic Key Pair, one private and one public, which securely identifies a device. Other devices such as a tablet, laptop and desktop can be similarly strongly authenticated (see pages 24-25). “Shared secrets" that can be stolen, intercepted and shared (like a mother’s maiden name, password, user id or where you went to elementary school) cannot be the basis for PayThat enrollment or authentication (see page 26). PayThat fully conforms with FFIEC guidance on End-User Authentication.
S.10.4: The PayThat authentication process, which is mandatory for all End-Users prior to accessing a PayThat CashBox, is accessed by the End-User through the PayThat software via one of two methods (see more detail on pages 31-33):

A. Single-sign on (SSO) using End-User’s existing Depository Institution mobile banking or internet banking services login authentication via a device that has been strongly authenticated and strongly enrolled as linked to the End-User; and

B. Direct sign-on using the authentication process of the identity management service called the Identity Assurance Federation (IAF).

End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices (see page 32).

S.10.5: PayThat uses the NIST 800-63-2 standard for enrollment and ongoing authentication. The level of assurance of identity proofing will rise from Level 1 to Level 4 per the NIST 800-63-2 standard based on risk and the dollar size of a proposed transaction (page 25).

End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices (see page 32).

Participants can optionally delegate the CashBox to automatically approve, or as a further option an approval upon confirmation by the End-User, requests for payments by recurring billing businesses. This combined with the automated reloading of good funds can ensure transactions are cleared if the End-User wants them to clear and has the funds available in any of (see page 30):

a. the End-User’s CashBox;
b. the End-User’s linked deposit accounts at their Depository Institution(s); and
c. End-User’s linked credit/line of credit accounts at their Depository Institution(s).

In this manner the current business model involving Pull Payments for businesses that bill End-Users monthly can be supported by the PayThat Payment System, however using a good funds model that avoids overdrafts and overdraft fees.

S.10.6: The authentication process of PayThat will incorporate the following foundational principles: … (7) Authentication methods will evolve over time based on the evolving threat landscape (see pages 33, 27).
Justification for S.11:

[Discuss self-assessment addressing considerations S.11.1 to S.11.3]

S.11.1: The PayThat Payment System rules that all Providers must agree and adhere to via a participation agreement, will ensure that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules, including those applicable to End-Users and that the PayThat Payment System can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures (see page 49). PayThat’s security (pages 48-49 and elsewhere), resiliency (page 48), AML/KYC (pages 14, 25, 32, 37, 39, 41, 46), data privacy (pages 26, 47-48), and data integrity rules (see pages 130 and 27-49) are each addressed in separate criteria.

S.11.2: The PayThat Payment System rules that all Providers must agree and adhere to via a participation agreement, will ensure that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules, including those applicable to End-Users and that the PayThat Payment System can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures (see page 49). Operational, liquidity and other risks specific to Depository Institutions are addressed in the PayThat rules, policies and procedures required on pages 48-49. The rules, policies and procedures are applied on a non-discriminatory basis to all Providers.

S.11.3: The PayThat Payment System rules that all Providers must agree and adhere to via a participation agreement, will ensure that the PayThat Payment System can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures (see page 49).

4. Speed (Fast)

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

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td># Consideration Name</td>
<td>VE E SE NE</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.1 Fast approval</td>
<td>X</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.2 Fast clearing</td>
<td>X</td>
</tr>
</tbody>
</table>
### In Pursuit of a Better Payment System

**Faster Payments Task Force**

<table>
<thead>
<tr>
<th>Speed (Fast)</th>
<th>F.3</th>
<th>Fast availability of good funds to payee</th>
<th>X</th>
<th>37, 33, 40</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed (Fast)</td>
<td>F.4</td>
<td>Fast settlement among depository institutions and regulated non-bank account providers</td>
<td>X</td>
<td>37, 36-37, 38-39, 1, 2 &amp; 3:44</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.5</td>
<td>Prompt visibility of payment status</td>
<td>X</td>
<td>41, 1 &amp; 2: 41</td>
</tr>
</tbody>
</table>

---

**Justification for F.1:**

[Discuss self-assessment]

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages should take under two seconds (see page 37).

**Justification for F.2:**

[Discuss self-assessment]

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages should take under two seconds (see page 37).

**Justification for F.3:**

[Discuss self-assessment]

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages should take under two seconds (see page 37). S-2 can authenticate to its CashBox in under 30 seconds (see page 33) and then have immediate access to the PayThat Tokens in the .pay file and have access to any contextual data it has a right to have access to, based on the privacy template adopted by S-1, and S-2’s role, authority, need to know and authenticated status, immediately upon receipt of Message #5. (see page 40).

**Justification for F.4:**

[Discuss self-assessment addressing considerations F.4.1 to F.4.3]

Assuming internet connectivity is not lost among the parties involved in a transaction (S-1, S-2, FI-1 and FI-2), the transmission and receipt of the eight payment messages should take under two seconds (see page 37).

Payer’s provider (FI-1) will actually settle the transaction and move the good funds from FI-1 to FI-2, or in the use case where S-2 also banks with FI-1, FI-1 will transfer the good funds from S-1’s account at FI-1 to S-2’s account at FI-1, when it has received the authenticated,
encrypted, untampered Message #1 and Message #3, and Message #6 has been received by FI-2 (or received by FI-1 in the alternative use case where FI-1 is also S-2’s Depository Institution) and FI-2 (or FI-1 in the alternative use case where FI-1 is also S-2’s Depository Institution) has informed FI-1 that Message #6 has been received. Individual transactions may be settled among Depository Institutions individually or in batch, on a net settlement basis, account to account, or via an existing legacy payment system such as FedACH or FedWire (pages 36-37).

Settlement may occur within two seconds if FI-1 and FI-2 have an agreement to settle each transaction immediately, or at a different interval agreed among them, to a maximum of 30 minutes. Smaller Depository Institutions to participate in the PayThat Payment System must join as a member of one of the limited number of PayThat Clearing Banks, one or more of which may be member owned by smaller Depository Institutions (pages 38-39).

F.4.1: Since the PayThat Payment System operates 24/7/365 and settlement via legacy ACH and Wire systems are not available on holidays and non-business days, the PayThat Payment System rules will require good funds to be held in central bank money escrow accounts in an amount designed by analysis and historical and projected flow of funds to ensure that sufficient funds are available to cover the net settlement risk among PayThat Clearing Banks and smaller Depository Institutions that are correspondents of PayThat Clearing Banks, to cover their obligations under Sigma 4, Sigma 5 or Sigma 6 probability, as determined by the PayThat Payment System rules (page 44).

F.4.2: PayThat Clearing Banks will be required to operate and continue settlement at extended hours to enable transactions in all time zones in the United States to have normal business hours in their own time zone (page 44).

F.4.3: PayThat Clearing Banks will be required to operate and continue settlement at extended hours to enable transactions in all time zones in the United States to have normal business hours in their own time zone. The PayThat Payment System rules will require good funds to be held in central bank money escrow accounts in an amount designed by analysis and historical and projected flow of funds to ensure that sufficient funds are available to cover the net settlement risk among PayThat Clearing Banks and smaller Depository Institutions that are correspondents of PayThat Clearing Banks, to cover their obligations under Sigma 4, Sigma 5 or Sigma 6 probability, as determined by the PayThat Payment System rules (page 44).

Justification for F.5:
[Discuss self-assessment addressing considerations F.5.1 to F.5.2]

All pending transactions are visible 24/7/365 in the Participant’s CashBox as pending authorized transactions. Specific details about pending status are also available including when their Depository Institution received and approved their payment request, when their Depository Institution account and CashBox has been debited, and when the payment was received by S-2 and cleared by FI-2 and FI-1 (page 41).

F.5.1: For S-1, this transaction detail would include when the payment was transmitted by them, when their Depository Institution received and approved the payment request, when
their Depository Institution account and CashBox has been debited, and when the payment was received by S-2 and cleared by FI-2 and FI-1 (page 41).

F.5.2: For S-2, this transaction detail would include when the payment was transmitted to them, when their Depository Institution received and approved the payment request, when their Depository Institution account and CashBox has been credited, and when the payment was received by S-2 and cleared by FI-2 and FI-1 (page 41).

5. Legal Framework

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: legal framework, payment system rules, consumer protections, data privacy, and intellectual property.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.1</td>
<td>Legal framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Legal Framework L.5 Intellectual property X 21

Justification for L.1: [Discuss self-assessment addressing considerations L.1.1 to L.1.5]

L.1.1: Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The following legal principles, rules and policies will be incorporated into these Governance Documents: All laws, regulations, regulatory interpretations or rulings, court decisions (collectively “Laws”) and/or PayThat Payment System Rules that will apply to the Payment System, End Users, Providers, Payers and Payees, and payments through the PayThat Payment System (page 50).
L.1.2: The PayThat Payment System is designed to operate within existing laws without any changes being required (page 50).

L.1.3: Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The following legal principles, rules and policies will be incorporated into these Governance Documents:
- Specificity as to how Entities and the payments themselves that transact through the PayThat Payment System will be legally bound to the PayThat Payment System Rules (page 50).

L.1.4: Compliance with various specific laws is discussed in detail: OFAC (page 25), BSA & AML (pages 14, 25, 32, 37, 39, 41, 42, 46, 73, 112, 114, 115, 117, 118), Regulation GG (page 25), Regulation E (pages 37-39, 41, 43, 46-48, 72), Regulation Z (page 48), MSB laws (page 25, 28, 32), all other applicable federal laws (page 50), all other applicable state laws (pages 49, 50).

L.1.5: Because the PayThat Payment System only allows Depository Institutions to become PayThat Clearing Banks, and Depository Institutions are all subject to the same regulations with respect to electronic payments, there are no instances where Providers are performing the same functions, but are subject to different applicable laws. Any legal issues with respect to End-Users where there are instances where Providers are performing the same functions, but are subject to different applicable laws will be addressed in the Governance Documents (see page 50-51).

Justification for L.2:
[Discuss self-assessment addressing considerations L.2.1 to L.2.5]

L.2.1: Topics in the list are discussed as follows:
- L.2.1.1 Authentication of all Entities, payments or messages connected to a payment (see pages 24-34);
- L.2.1.2 Legal responsibility of Providers that provide Payment System access to End Users (see #1, #2, #3, #4, page 50);
- L.2.1.3 Payment Order Initiation/Authorization (see pages 29-36) and termination of Authorization (see page 35);
- L.2.1.4 Cancellation of a Payment (see page 35);
- L.2.1.5 Delayed and failed payments (see page 43, 47-50);
- L.2.1.6 Payment Finality (pages 41 and 36-39, 54, 55) and Settlement (see pages 43-44);
- L.2.1.7 Timing of sending and receipt of a payment (pages 38, 39, 41, 44);
- L.2.1.8 Records as proof of payment for Payers and Payees (see #4, page 50); and
- L.2.1.9 Error Resolution for anticipated disputed payments among End Users, Providers, Payers and Payees (see #4, page 50).

L.2.2: The governance model, voting and amendment process by class of Entity and the process for obtaining input from PayThat Payment System stakeholders will be drafted within six months of the commencement of initial work to build PayThat (see #5, page 50).
L.2.3: The PayThat Payment System shall have the authority to examine and audit Entities and sanction and if necessary expel them from the PayThat Payment System (see #4, page 50).

L.2.4: The allocation of losses due to the failure by the IAF, a Depository Institution or a PayThat Clearing Bank to properly vet End-Users during enrollment and authorization will be drafted within six months of the commencement of initial work to build PayThat (see #6, page 50).

L.2.5: Codification into specific written rules of the PayThat Payment System Rules regarding … the error resolution process … as described in this document will be drafted within six months of the commencement of initial work to build PayThat (see #4, page 50).

Justification for L.3:

[Discuss self-assessment addressing considerations L.3.1 to L.3.3]

L.3.1: 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 will be drafted within six months of the commencement of initial work to build PayThat (see #1, #2, #3, #4, #6 page 50). To the extent feasible the legal framework will follow Regulation E (pages 37-39, 41, 43, 46-48, 72) or Regulation Z (page 48), with respect to consumer rights, obligations and liability.

L.3.2: Payment System Rules and procedures that support Error Resolution for Consumer claims arising from payments Fraud, unauthorized payments or errors as described in this document will be drafted within six months of the commencement of initial work to build PayThat (see #1, #2, #3, #4, #6 page 50). To the extent feasible the legal framework will follow Regulation E (pages 37-39, 41, 43, 46-48, 72) or Regulation Z (page 48), with respect to consumer rights, obligations and liability.

L.3.3: Rules under which PayThat Clearing Banks or the PayThat Payment System itself may optionally establish for End Users and/or Providers additional Consumer protections for payments, which may exceed those protections that are otherwise required under applicable law will be drafted within six months of the commencement of initial work to build PayThat (see #7, page 50).

Justification for L.4:

[Discuss self-assessment addressing considerations L.4.1 to L.4.5]

1. L.4.1: In the PayThat Payment System Data is ubiquitous & access controlled, controlled only by users, utilizing standard privacy templates by ecosystem (see page 13). The PayThat Payment System supports privacy templates where users can mandate who has access to data by role and authority (see page 13, 16). At enrollment, participants selected a privacy template level of high, medium or low. These privacy templates can be fine tuned to the specific needs of industry ecosystems, e.g. healthcare for HIPAA requirements. In the privacy template users can mandate who has access to data by role and authority. With a high privacy template setting a degree of anonymity can be assured for participants.
Merchants may incentivize participants to select a low or medium privacy template to enroll in additional value added services, such as loyalty point programs (page 27).

L.4.2: PayThat uses a cash purse system enhanced with end to end encryption of data at motion and at rest (see pages 9, 11, 12, 15, 16, 26, 33, 35-37, 39-40, 42, 46, 48, 49, 55, 61, 65, 72, 74, 76-77, 86-87, 109-110, 120, 122).

PayThat uses a “Data-Centric” approach to encryption: data access is controlled by role & authority on a transaction level basis and by individual field or record; access controlled by End-users’ privacy templates, established at the edge servers at the nodes. Access to all data is controlled by rules enforced by strong encryption, providing greater control & security. Data is persistently secured and encrypted, so that data can travel freely across the cloud, databases or insecure systems/networks as an encrypted, secure data element and still be access controlled based on role and authority as governed by the End-User’s privacy template. Access is controlled by role, authority, need to know and only for the duration that it is needed to be known.

Key customer data is NOT shared with merchants or others unless needed or authorized by customers (pages 12-13).

The .pay file uses cryptographic standards so that each data element is separately encrypted such that data elements are accessible solely and variably based on role, authority, authentication status and need to know (page 15). The .pay file uses cryptographic standards so that each data element is separately encrypted such that data elements are accessible solely and variably based on role, authority, authentication status and need to know (page 16).

If some fraud, Regulation E related issues, AML or BSA issues has been detected or reported or a request from law enforcement is received to block an account to FI-1 or FI-2, either or both of FI-1 or FI-2 may reset the funds in S-1’s and/or S-2’s accounts or block funds in S-1’s or S-2’s accounts as necessary (page 37, 41).

The PayThat payment system will accumulate PII data in an encrypted database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only (page 26).

Research of the pending transactions and cleared transactions by law enforcement and the Federal Reserve’s economic research unit can be facilitated based on role, authority and a need to know. For example, law enforcement may need to know the identity of the End-Users involved in a transaction but not some data elements about some transactions, such as health-care related data controlled by HIPAA related to heart surgery. Those data elements could not be unlocked for research purposes without a judge’s court order digitally signed granting them authority based on need to know. The Federal Reserve’s economic research unit could gain access to real-time data on transaction sizes and goods being sold across the economy but not need to know the identity of the End-users involved in the transaction. Those data elements would remain encrypted and not be accessible to the researchers based on their lack of a need to know (page 46).

All data in the four PayThat Payment System Databases shall be stored for seven years to facilitate research in line with the needs of industry to research tax related issues related to payments. After seven years, the encrypted data elements cannot be accessed regardless of...
role, authority or a need to know. Optionally, some data elements may have a shorter shelf life if the PayThat Payment System rules require it in compliance with applicable laws and regulations (page 48).
L.4.3: PayThat will collect PII during the enrollment process. PII will not be used to authenticate transactions once an End-User is strongly enrolled. The PayThat payment system will accumulate PII data in an encrypted database where all data is encrypted at motion and at rest and access is provided on a need to know basis, based on role, authority and authentication status only. The IAF will utilize this data to authenticate End-Users when engaged in transactions or error resolution processes (page 26). Research of the pending transactions and cleared transactions by law enforcement and the Federal Reserve’s economic research unit can be facilitated based on role, authority and a need to know. For example, law enforcement may need to know the identity of the End-Users involved in a transaction but not some data elements about some transactions, such as health-care related data controlled by HIPAA related to heart surgery. Those data elements could not be unlocked for research purposes without a judge’s court order digitally signed granting them authority based on need to know. The Federal Reserve’s economic research unit could gain access to real-time data on transaction sizes and goods being sold across the economy but not need to know the identity of the End-users involved in the transaction. Those data elements would remain encrypted and not be accessible to the researchers based on their lack of a need to know (page 46).
L.4.4: End-users may obtain a report detailing the data collected about them under the terms of the privacy template they adopted as modified from time to time (page 27).
L.4.5: All nodes in the PayThat Payment System will be protected by state of the art cyber security protection, monitoring and malicious pattern detection systems that perform and facilitate data breach prevention and detection. For example, the Promia Raven, which protects the data centers of the U.S. Navy’s Network Operating Centers, would be a good candidate vendor solution, however the actual system would be selected following an RFP. The IAF will manage the cyber security protection, monitoring, malicious pattern detection and data breach prevention and detection systems for the four databases, as well as data breach reporting for the PayThat Payment System, the IAF and the PayThat Clearing Banks (page 48).
Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that allocate losses due to the failure by the IAF, a Depository Institution or a PayThat Clearing Bank to properly vet End-Users during enrollment and authorization or due to a data breach (page 50, #6).

**Justification for L.5:**

*Discuss self-assessment addressing consideration L.5.1*

Within six months of the commencement of initial work to build PayThat, an intellectual property search by a nationally recognized law firm specializing in intellectual property will
be performed to determine a strategy to resolve or manage, prior to implementation, any legal, operational or financial risks to the Payment System, End Users and Providers arising from third-party intellectual property rights (including patents, trademarks, copyrights and trade secrets). To date, University Bank has only undertaken a partial due diligence investigation of potentially applicable intellectual property rights to the PayThat proposal, with the result that the patents listed in this section have been identified. A significant amount of University Bank owned intellectual property has been incorporated into this copyrighted document (page 21).

6. Governance

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

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Governance</td>
<td>G.1</td>
<td>Effective governance</td>
</tr>
<tr>
<td>Governance</td>
<td>G.2</td>
<td>Inclusive governance</td>
</tr>
</tbody>
</table>

**Justification for G.1:**

[Distinguish self-assessment addressing considerations G.1.1 to G.1.4]
Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The enumerated legal principles, rules and policies in G.1.1, G.1.2, G.1.3 and G.1.4 will be incorporated into these Governance Documents. (see page 50, #5)

**Justification for G.2:**

[Distinguish self-assessment addressing considerations G.2.1 to G.2.5]
G.2.1: Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The enumerated legal principles, rules and policies in G.2.1, G.2.2, G.2.3, G.2.4 and G.2.5 will be incorporated into these Governance Documents. (see page 50, #5)
Author’s Final Thoughts Regarding PayThat & Faster & More Secure Payments

My purpose in putting forth this proposal is to get a dialogue started so that we can begin to solve the many vexing problems facing our banks. Many of these problems have been around for over twenty years and growing in importance with no resolution in sight, yet the risks and dangers are growing by the week. In approaching this topic, we are reminded of the famous quote from Lord Maynard Keynes:

“Perhaps you will think the proposals too ambitious, too idealistic, altogether too grand. But isn’t this a merit?”

This thought is tempered by the conventional thinking about entrepreneurs in the banking industry. Conventional wisdom in banking says:

“Pioneers get the arrows, and settlers get the land!”

But, in the land of Technology: Pioneers buy the land for 40 bucks an acre at the Government Land Office and charge rent to everyone who shows up later (a/k/a The Early Mover Advantage).

With the rising risks to our institutions growing rapidly, Ben Franklin perhaps has the solution:

“We must all hang together, or assuredly we shall all hang separately.”

The solutions to these problem cannot be solved by one institution acting alone. Together we can create the network effect required to launch robust solutions into the marketplace. What is needed?

I think we would be successful if we architect and build a new payment system were all users are strongly enrolled, where all data is encrypted end to end at all times and never in the clear, in motion and at rest, and all access to data is tightly controlled based on authentication, role, authority and a need to know.

A payment system that meets those criteria will produce many positive benefits to society, including the elimination of the identity theft criminal ecosystem, the creation of many new jobs, better access to financial services by the unbanked, and the elimination of the need for consumers to remember passwords when transacting on websites across the Internet.

I like my ideas but I want to see something finally get done! I’ll adopt your better ideas and help you bring them to fruition, if that is what it takes to get a Real-Time Highly Secure Payment System built and deployed for our mutual benefit. It’s your turn to put your ideas on the table.
Faster Payments QIAT

PRELIMINARY ASSESSMENT

Proposer: University Bank

COMMENTS BY PROPOSER ON PRELIMINARY ASSESSMENT

Using the four innovative adoption use cases detailed in the Proposal (see pages 75-123), each PayThat Clearing Bank would for a modest investment to purchase a license, own a fee driven business that for each of the eight licensees would be worth $3.58 billion to $4.1 billion within three years if they achieve average market share of 12.5%. Since the PayThat Corporation would be worth $940 million to $1.55 billion (see page 104 of the Proposal), the entire PayThat Network would be worth $29.58 billion to $34.35 billion. Please see the Question and Answer to E.3.1 on page 6 below for more details.

McKinsey’s initial reviewers had a fundamental misunderstanding of PayThat prior to the QIAT Q&A conference call. PayThat is based on a system of End-User controlled cash purses each called a PayThat CashBox, run by a new “network of networks” that interoperates with however is separate from the existing bank deposit, bank payment, and bank clearing systems. This “network of networks” is called PayThat Clearing Banks in the proposal. Once money is transferred into a cash purse held by a customer of a PayThat Clearing Bank, it remains there allowing transactions to be settled natively inside a single and among the several PayThat Clearing Banks real-time, in a fraction of a second. No funds are ever required to be transmitted or settled via traditional bank payment systems such as ACH, Wire, ATM Debit networks & etc.

If a customer instructs its bank to transfer money into their PayThat account that money is held on deposit by a PayThat Clearing Bank in a linked traditional bank account controlled by the PayThat Clearing Bank, however that deposit is blocked and not available to the customer, unless and until the customer instructs the PayThat Clearing Bank to transfer the funds back to their linked traditional bank account. This may never happen, since the customer may opt to conduct all their financial transactions in the PayThat network. PayThat Clearing Banks only hold and transact good funds and operate on a 1:1 basis: for each PayThat Token in existence, there is 100% of the good funds represented by that PayThat Token on deposit at a traditional bank account controlled by the PayThat Clearing Bank.

If a customer instructs its PayThat Clearing Bank to withdraw funds from their PayThat CashBox and transfer those funds back to a traditional bank deposit account, this transfer is carried out by the PayThat Clearing Bank by issuing an account transfer request to its linked bank that holds its blocked good funds deposit account, to transfer those funds from the PayThat Clearing Bank’s deposit account to the customer’s traditional bank account. This is a purely optional step and not needed unless the customer wishes to withdraw good funds from their PayThat CashBox.
Since the PayThat system of PayThat Clearing Bank is built on top of and interoperates with the existing bank deposit, bank payment, and bank clearing systems, it can facilitate adoption while coexisting with these legacy bank systems. Over time as PayThat adoption reaches a critical mass, the End-Users’ need to move funds back to the legacy bank systems will diminish and ultimately these systems will be able to be sunset when it makes financial sense to the financial institutions to do so.

The best practice to achieve strong enrollment and strong authentication is to start at a commercially reasonable initial lower level of enrollment and authentication and then require customers to jump over additional hurdles when they wish to perform a transaction that poses more risk that the risk model allows without increasing the assurance of identity and authentication status. Customers have a high willingness to comply with additional requirements if they have a pending transaction that they wish to complete. As noted on pages 25 & 32-33 of the proposal:

“End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers, or prohibited transactions, such as a gambling transaction prohibited by Regulation GG). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices.”

**APPENDIX A: QUESTIONS BACK TO PROPOSER**

**Ubiquity**

- **U.1.5:** May the assessment team see the proposal that is available under MNDA so that we may better understand how the solution would resolve the unbanked issue?

  This information is available to any party willing to sign University Bank’s standard MNDA. Please contact President Stephen Lange Ranzini at ranzini@university-bank.com to request a copy. The Prime Minister of India has implemented a solution based on PayThat and PayThat’s business model for a new national payment system and national identity management system that already has resulted in over 600 million new bank accounts being adopted by the unbanked population of India and a national identity management system substantially similar to the proposed PayThat Identity Assurance Federation (IAF) described in the proposal.

- **U.2.1:** Can PayThat be used to purchase online or at the point of sale (POS)? For online or POS purchases, how would the email/SMS be tied to the transaction? How would a user request payment? If these use cases cannot be easily supported, an end-user will have to have two accounts: a PayThat CashBox and a regular bank account.

  Yes, PayThat be used to purchase online or at the point of sale (POS) via email (SMTP) or SMS (text message) rails. It can be integrated into any existing merchant acquiring solution or implemented as a separate work-around. For example, under MNDA University Bank
provided such a solution to the National Association of Convenience Stores (NACS). PayThat can run using the same mobile device based POS rails and would have the same challenges as mobile payment systems already tested and deployed. Under MNDA University Bank also provided a design for an vehicle centric version of PayThat to a Big Three Automaker that requested University Bank to deploy PayThat tied to a vehicle key fob and interoperating through the vehicle’s operating system “bus” which is tied to a cellular data network.

U.4.1: Does the solution allow for data fields that are specific to industry verticals? Can it support expanded remittance needs for B2B payments? Please provide more detail on how data is captured and shared, as well as what can be included in the data.

Yes, PayThat supports the version of XML based on the global standard United Nations CEFACT XML Data Dictionary. UN CEFACT has developed XML global standards for each industry vertical fine tuned to the specific needs of each industry vertical. These UN CEFACT standards are adopted by law in all but a few countries around the world, the U.S. being one of the few notable countries that has not mandated and required all industry and government to use solely the UN CEFACT Data Dictionary. ISO20022 has also been adopted into and harmonized with the UN CEFACT Data Dictionary. Stephen Lange Ranzini was the U.S. banking industry representative to UN CEFACT from 2003 to 2011. The UN CEFACT Data Dictionary supports all known requirements for expanded remittance needs for B2B payments. XML Data is captured and shared using the “network of networks” architecture and APIs to standard ERP packages such as Oracle, SAP and Microsoft ERP systems, including Excel and Dynamics. SEMHIE developed a health care industry specific data dictionary that allows seamless translation of ICD-10 and ICD-9 information into Snowmed and other preferred XML data formats.

U.4.2: Can this solution do everything that ISO 20022 can do? Please describe the solution’s interfacing functionality.

Yes, ISO20022 is XML based. PayThat supports the version of XML based on the global standard United Nations CEFACT XML Data Dictionary. ISO20022 has also been adopted into and harmonized with the UN CEFACT Data Dictionary. XML Data is captured and shared using the “network of networks” architecture and APIs to standard ERP packages such as Oracle, SAP and Microsoft ERP systems, including Excel and Dynamics.

Another excellent method of interoperating expanded remittance needs for B2B payments is a system developed by NACHA’s EBIDS (Electronic Billing Information Delivery Service) committee, which Stephen Lange Ranzini, the Federal Reserve Bank System and others helped develop and is now owned and managed by The Clearing House. This system allows seamless interoperability with standard bank bill payment and internet banking systems in support of expanded remittance needs for B2B and B2C payments and invoicing.

The “payment kernel” of ISO20022 is embedded in the cryptographic object inside the PayThat Tokens.

U.4.2: Please describe how this interfacing will work. How easy is the solution to integrate? Does it require substantial configuration?
PayThat does not require substantial configuration because it uses the “network of networks” architecture described on pages 120-123. If a software system or an API of the system can handle XML tagged data, interfacing with the PayThat data is an inexpensive and cost effective process.

■ U.4.3: How do parties with different messaging capabilities avoid losing contextual data in the translation from one standard to another?

This is a common problem with XML based systems and the key reason why XML standards and XML Data Dictionaries are important. Tools to automate the API map debugging process are widely deployed in industry that allow a real-time view that is human readable of what the input and output of an XML translation map is as individual elements of a map are, when changed during the debugging process.

■ U.5.2: Please provide more detail on how the solution is interoperable with other countries’ payment systems, beyond its support for ISO 20022.

See the detailed description of the Global Payment Gateway on pages 54-57 of the Proposal, the summary of which is as follows:

“The Global Payment Gateway (GPG) is a web service built by Depository Institutions that communicates through and leverages legacy payment networks in each country around the world to enable cross-border payment functionality in real-time leveraging RTGS payment systems around the world. The concept was first piloted in the Universal Value eXchange (UVX) pilot of the Financial Services Technology Consortium (FSTC). Several major banks have since built GPGs including Wells Fargo and Chase Bank. The PayThat Payment System would either utilize one or more of the existing GPGs selected by RFP, or build a new one in partnership with a large bank selected via RFP.” Stephen Lange Ranzini was the Deputy Project Manager for the FSTC UVX Pilot.

■ U.5.4: Who sets the solution’s exchange rates?

This is an optional Value Added Service provided by the PayThat Clearing Banks to the customers of the PayThat Clearing Banks.

Efficiency

■ E.1: Is the 8 clearing licenses a hard limit or is it extensible?

More licenses could be created. The rationale for limiting the number of licenses is based on a desire to accelerate adoption using the “First Mover Advantage” and the “Too late, you weep” principles.

■ E.1: What are the criteria for choosing which Financial Institutions are awarded the 8 clearing licenses?

If demand is high, it would be based on an RFP process based on which specific proposals would accelerate and drive adoption most rapidly. At least one license will be held in reserve for a consortium of Small Financial Institutions and/or a Bankers Bank and/or a CUSO primarily serving Small Financial Institutions.

■ E.1.4: Is there an operating cost or service offering differential (such as service delays) for small FIs, given that they are working through a hosted clearing bank?
Small Financial Institutions can purchase access to PayThat services for their customer base either through a large correspondent bank that owns a PayThat Clearing Bank or through the (at least) one PayThat Clearing Bank license reserved for a consortium of Small Financial Institutions and/or a Bankers Bank and/or a CUSO serving Small Financial Institutions. While a profit margin will be built into their business model, the typical bankers’ bank operates on a 5% Return on Equity business model, so the additional cost is modest. Competitive pressure from the eight licensees fighting for market share will encourage correspondent PayThat Clearing Banks to offer fair prices for access to PayThat services. There would be no service delays for small FIs working through a correspondent PayThat Clearing Bank.

E.2.1: Please explain in detail the implementation requirements for Clearing Banks to how providers integrate with the solution.

Please see the discussion regarding “integration effort” on pages 120-123 of the Proposal. The summary is as follows:

“In the PayThat use cases, the only points of integration are between the PayThat Clearing Banks, which serve as “edge servers” for traditional Depository Institutions and the payment systems of those traditional Depository Institutions. The integration required is equivalent to a banking corporate treasury workstation. The integration is modest and should only take weeks. By design and purposefully the amount of IT integration with the systems of legacy Depository Institutions is kept to a minimal level. Since most corporate treasury workstation solutions support data exporting and data importing, the challenge is mostly reduced to mapping and by using state of the art mapping automation tools, which have low six figure costs, the technical challenge is low and the technical risk is low. The only point at which there is a point of integration in the eight stages of the payment lifecycle (as discussed in Part A) is when good funds are to be loaded into PayThat or taken out of PayThat. This is as simple as a credit or debit message using the corporate treasury workstation between the traditional Depository Institution and the PayThat Clearing Bank. All the other functions occur within the new PayThat Payment System network, and are described elsewhere in detail.”

E.3.1: Please identify the target Clearing Banks. Why has the number of licenses been capped at 8 for the U.S., as well as why partnership with PayThat would be attractive to them? How many clearing partners can the solution support?

Any of the top 100 U.S. banks or equivalent size credit unions would be an ideal candidate to purchase a PayThat Clearing Bank license. The licenses will be sold on a first-come first served basis unless demand is high. If demand is high, allocation would be based on an RFP process based on which specific proposals would accelerate and drive adoption most rapidly. At least one license will be held in reserve for a consortium of Small Financial Institutions and/or a Bankers Bank and/or a CUSO serving Small Financial Institutions.

Each PayThat Clearing Bank would for a modest investment to purchase a license, own a fee driven business that for each of the eight licensees would be worth $3.58 billion to $4.1 billion within three years if they achieve average market share of 12.5%:

- Use Case #1 is worth at least $1 billion for the PayThat enabled Health Information Exchange payment system proposal as the PayThat HIE services will capture a portion
of the $4.5 billion off administrative costs for doctors and hospitals, private health plans, states and other government health plans that HHS has estimated can be saved by adoption of such a system over the next 10 years (see pages 75 & 79 of the Proposal).

- Use Case #2 Each PayThat Clearing Bank would own a fee driven business that would have a value of between $780 million and $1.30 billion at the end of the third year after the launch of the First Class Email product (see page 106 of the Proposal).

- Use Case #3 is worth at least $1 billion for the Single Window for Cross Border Trade Facilitation & Supply Chain Billing (see pages 108-112 of the Proposal).

- Use Case #4 is worth $10.2 billion for the credit bureau alone and likely at least double that for the IAF (see page 114 of the Proposal).

Since the PayThat Corporation would be worth $940 million to $1.55 billion (see page 104 of the Proposal), the entire PayThat Network would be worth $29.58 billion to $34.35 billion.

E.3.1: The enrollment process seems onerous. How will the proposer engage consumers to complete the steps required for Level 4?

The best practice to achieve strong enrollment and strong authentication is to start at a commercially reasonable initial lower level of enrollment and authentication and then require customers to jump over additional hurdles when they wish to perform a transaction that poses more risk that the risk model allows without increasing the assurance of identity and authentication status. Customers have a high willingness to comply with additional requirements if they have a pending transaction that they wish to complete. As noted on pages 25 & 32-33 of the proposal:

“End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers, or prohibited transactions, such as a gambling transaction prohibited by Regulation GG). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices.”

E.3.1: Please provide more details on the plan and timeframe to secure funding to meet the 18-month timeline for launch.

Since the PayThat Corporation would be worth $940 million to $1.55 billion (see page 104 of the Proposal), and because the cost to build the four use cases targeted by the PayThat Payment System is under $100 million, this is an attractive venture capital opportunity. Following the issuance to the general public of the results of the Federal Reserve Faster Payments RFP whitepaper, venture capital procurement efforts and licensing will commence. The capital raising process should be completed within four months of initiation. To the extent that there are early adopter licensees who purchase PayThat Clearing Bank licenses, the capital raise required from the venture capital industry would be reduced by those license fees.
E.6.2: What are the proposer’s volume projections for the system? How does the proposer plan to accommodate these volumes? What is the buffer for peak times? Can the proposer describe the cycle for stress-testing volume spikes?

Ultimately, the volume of the system will be comparable to VISANet, which we understand currently settles 24,000 transactions per second, and this will grow with the economy over time, however, since there are only eight PayThat Clearing Banks and on-us transactions will be settled inside each PayThat Clearing Bank, much of the volume will not occur between PayThat Clearing Banks but inside PayThat Clearing Banks. The system messaging which is based on SMTP and SMS standards, which currently can easily handle millions of transactions a second, scales well and could easily accommodate 100,000 simultaneous transactions according to an analysis by one of the architects of the PayThat System, Chris Weideman, the former CTO of Chrysler Financial. Quarterly testing using micropayments each worth $0.0001 will be conducted at rates 20x the historic peak transaction rates of the system to ensure it is always able to handle a large surge in transaction volume.

E.7.1: How will the Postal Service’s security arm scale to handle the volume of enforcement requests?

The USPIS currently has 1,200 employees and is generally regarded as the most effective financial fraud investigative and enforcement agency in the U.S. The leadership of the organization has informally assured me that they are eager to expand and take on the role proposed for it in the Proposal. Its current systems are readily scalable. It is much easier to scale up an existing business than to start a new one from scratch.

E.7.1: While "investigations" by FIs and return of funds are outlined, will the solution provide any tools or protocols for parties—particularly end-users and providers—to address exceptions?

As noted in the Proposal, the PayThat Clearing Banks will use existing institution specific tools and protocols. See pages 26, 37, 39, 41, 42, 46, 47, 48, 52, 70, 73, 77, 80, 85 and 98 of the Proposal as noted on page 131.

E.7.1: On page 48, the proposer states that FIs will use “existing standard error resolution process under Regulation E and in the timeframes currently applicable.” For ACH and wire transactions, these processes generally occur during bankers’ hours. How will PayThat handle error resolution in a 24x7x365 environment?

The PayThat Clearing Banks will be required to expand these existing business units that handle End-User error resolution to a three shift, 24x7x365, operation.

E.7.3: Is exception data aggregated across FIs in a comprehensive database?

Yes, and all access will be based on role, authority, authenticated status and a need to know. As noted on page 137:

“S.6.3: The IAF will be responsible for facilitating timely and frequent sharing of information among all Providers, operators and regulators to help them manage, monitor, and mitigate Fraud and evolving threats in accordance with applicable law (see pages 47-48). The four databases include aggregated data from each step of the business process from authentication to pending transactions to cleared transactions.”

Please also see the discussion of the four databases on pages 46-48 of the Proposal.
E.7.3: Will exceptions be handled similarly to fraud items? Who will be responsible for the analysis and insights?

Analysis and insights will be performed by PayThat Clearing Bank staff or staff of the bank licensee of the PayThat Clearing Bank. The IAF will also perform analysis and share insights with the PayThat Clearing Banks as noted on pages 48-49:

“The IAF will manage the cyber security protection, monitoring, malicious pattern detection and data breach prevention and detection systems for the four databases, as well as data breach reporting for the PayThat Payment System, the IAF and the PayThat Clearing Banks.”

See the discussion that follows this sentence.

The USPIS will also perform analysis and share insights with the IAF and the PayThat Clearing Banks performed in their role as the identity fraud law enforcer for the IAF and PayThat Payment System.

E.7.2-E.7.3: How will this solution monitor transactions across accounts/clearing banks to identify suspicious patterns? Does the solution include tools that will allow Clearing Banks to search PayThat data bases to support fraud and exception management?

PayThat Clearing Bank and Bank licensees can use existing tools to analyze and identify suspicious patterns. The PayThat data will just be another (XML) data feed for their existing tools. For more details, see page 49, bullets 2, 4 &5 and page 50, bullet 1 of the Proposal.

Safety and Security

S.1.2: How is institutional settlement risk addressed?

PayThat Clearing Banks only hold and transact good funds and operate on a 1:1 basis: for each PayThat Token in existence, there is 100% of the good funds represented by that PayThat Token on deposit at a traditional bank account controlled by the PayThat Clearing Bank. Settlement inside the PayThat Payment System is continuous and real-time both for on-us transactions inside a single PayThat Clearing Bank and for transactions involving two PayThat Clearing Banks.

S.1.5: Please describe the incentives for operators to manage the risk they may pose to other participants.

As noted on page 50 of the Proposal, the PayThat Payment System shall have the authority to examine and audit Entities and sanction and if necessary expel them from the PayThat Payment System for material uncorrected failures to adhere to the network rules.

S.1.6: How frequently will the risk management framework undergo review?

Annually or more frequently if needed. See page 50, bullet 2 of the Proposal.

S.4.1: Is the proposer suggesting that transactions be settled individually? If so, what is the plan for the FRB to upgrade the capability of the NSS [National Settlement Service] to handle this?

Not applicable, as the premise of this question is in error. McKinsey’s initial reviewers had a fundamental misunderstand of PayThat prior to the QIAT Q&A conference call. PayThat is based on a system of cash purses each called a PayThat CashBox, run by a new “network of networks” that interoperates with the existing bank deposit, bank payment, and bank clearing systems. This “network of networks” is called PayThat Clearing Banks in the proposal.
Once money is transferred into a cash purse held by a customer of a PayThat Clearing Bank, it remains there allowing transactions to be settled natively inside a single and among the several PayThat Clearing Banks real-time, in a fraction of a second. No funds are ever required to be transmitted or settled via traditional bank payment systems such as ACH, Wire, ATM Debit networks & etc.

If a customer instructs its bank to transfer money into their PayThat account that money is held on deposit by a PayThat Clearing Bank in a linked traditional bank account controlled by the PayThat Clearing Bank, however that deposit is blocked and not available to the customer, unless and until the customer instructs the PayThat Clearing Bank to transfer the funds back to their linked traditional bank account. This may never happen, since the customer may opt to conduct all their financial transactions in the PayThat network. PayThat Clearing Banks only hold and transact good funds and operate on a 1:1 basis: for each PayThat Token in existence, there is 100% of the good funds represented by that PayThat Token on deposit at a traditional bank account controlled by the PayThat Clearing Bank.

If a customer instructs its PayThat Clearing Bank to withdraw funds from their PayThat CashBox and transfer those funds back to a traditional bank deposit account, this transfer is carried out by the PayThat Clearing Bank by issuing an account transfer request to its linked bank that holds its blocked good funds deposit account, to transfer those funds from the PayThat Clearing Bank’s deposit account to the customer’s traditional bank account. This is a purely optional step and not needed unless the customer wishes to withdraw good funds from their PayThat CashBox.

Since the PayThat system of PayThat Clearing Bank is built on top of and interoperates with the existing bank deposit, bank payment, and bank clearing systems, it can facilitate adoption while coexisting with these legacy bank systems. Over time as PayThat adoption reaches a critical mass, the End-Users’ need to move funds back to the legacy bank systems will diminish and ultimately these systems will be able to be sunset when it makes financial sense to the banking industry to do so.

- S.4: Could PayThat clearing banks use real-time networks like The Clearing House for settlement? If so, how?
  Yes, however this is not recommended. The Clearing House could certainly purchase a PayThat Clearing Bank license, if they wanted to.

- S.5.4: If existing FI processes are used in what is purportedly a real-time system, how will the solution handle timing over weekends and holidays?
  Not applicable, as the premise of this question is in error, as noted above. See the answer to S.4.1 on page 9.

- S.5: How much integration and training will be required for clearing FIs to support customer complaints, fraud, and Regulation E issues related to PayThat?
  The training and integration required to support customer complaints, fraud, and Regulation E issues related to PayThat will be comparable to any new typical product roll-out at a Financial Institution (other than a residential mortgage product, which is much more complex).
S.5: How will customer service representatives be granted visibility into the Cashbox/PayThat databases to review transaction history and to provide assistance to customers?

All access to data in the four databases will be based on role, authority, authenticated status and a need to know. Database queries will provide back responses based on role, authority, authenticated status and a need to know. Need to know includes there being an active customer service ticket which is not yet resolved.

S.6.1: How frequently will fraud information be shared? Is this capability real-time?

Yes.

S.6.1: Is the fraud information database updated in real time? Can providers access the data for real-time fraud inquiries if they desire?

Yes, based on role, authority, authenticated status and a need to know.

S.6.3: Could the capabilities of the IAF be expanded to provide centralized fraud monitoring?

Yes, this is intended in the Proposal.

S.6.7: Please describe how exceptions data will be aggregated and analyzed.

Data will be tagged with XML tags and shared using the “network of networks” architecture described on pages 120-123 of the Proposal. PayThat Clearing Bank and Bank licensees can use existing tools to analyze and identify suspicious patterns. The PayThat data will just be another (XML) data feed for their existing tools. For more details, see page 49, bullets 2, 4 &5 and page 50, bullet 1 of the Proposal.

S.8.1: Please describe the proposer’s approach to maintaining the solution’s target availability metrics.

The PayThat Payment System will ensure its target availability by ensure adherence to the best practices listed on pages 49 and 50 of the Proposal.

S.8.4: What level (e.g., number, resources’ expertise, etc.) of specific resources is needed to ensure business continuity and resiliency?

To answer this question appropriately would require detail from the implementation and build-out phase of the Proposal, which is not yet available. The cost will be reasonable and manageable and comparable to a state of the art secure IT operations center found at any medium size Financial Institution. Over time the resources will grow as network volume and End-User adoption rises so that the resources will be comparable to what is available to a large size Financial Institution.

S.8.5: How frequently will “periodic” contingency testing of PayThat systems occur?

This will differ based on the criticality of the risk as identified in the enterprise risk management program and assessment. Some could be daily, weekly, monthly, quarterly or annually.

S.9.1: How will end-users’ data be encrypted? Will specific encryption standards will be deployed?

ASC-X9 Encryption Standards will be used to encrypt end-users data using methods known as Digital Rights Management, or as we prefer to refer to it, Persistent Digital Security (PDS).
Speed (Fast)

- F.4.1: How will FIs settle in central bank money immediately with the exchange of payment messages?
  PayThat Clearing Banks will settle between themselves using the blocked funds on deposit at their correspondent bank. Transactions internal to a PayThat Clearing Bank (on-us transactions) will settle immediately on the ledger of the PayThat Clearing Bank.

- F.4.1: Will the central bank need to support individual transaction settlement?
  No.

- F.4.3: Can banks settle in real time, if required? Please explain how real-time settlement would work in the PayThat system.
  PayThat Clearing Banks will always settle in real-time, unless they agree among themselves to some other method. See the answer to S.4.1, above.

Legal

- L.1.2: The proposal states that “the PayThat payment system is designed to operate within existing laws without any changes being required” (page 148). Please provide detail as to how legal gaps, if any, would be addressed.

  As stated on page 148 of the Proposal: “The PayThat Payment System is designed to operate within existing laws without any changes being required (page 50).” Since the PayThat Payment System would be operated by banks, any gaps in legal authority could be eliminated via the standard bank application process for initiating new banking activities. This generally results in an answer from banking regulators within 90 days. Banks generally have wide authority for financial services related activity, so it is unlikely that there would be any major hurdles. The PayThat Payment System Governance Documents would also be able to define requirements where there is no definitive legal guidance currently in place. The Governance Documents will bind all the Providers and End-Users of the PayThat Payment System (see page 147).

- L.1: Please provide more details regarding the Legal Framework that will govern the Solution’s operation and/or impose any compliance obligations on the Solution or End Users. In doing so, please specifically address how the Solution supports the five Legal Framework subcriteria.

  L.1.1: As noted on page 147 of the Proposal, “Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The following legal principles, rules and policies will be incorporated into these Governance Documents: All laws, regulations, regulatory interpretations or rulings, court decisions (collectively “Laws”) and/or PayThat Payment System Rules that will apply to the Payment System, End Users, Providers, Payers and Payees, and payments through the PayThat Payment System (page 50).” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional
decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.1.2: The PayThat Payment System is designed to operate within existing laws without any changes being required (see page 50 of the Proposal). There are no known gaps in legal authority.

L.1.3: The Governance Documents will bind all the Providers and End-Users of the PayThat Payment System (see page 147 of the Proposal). Acceptance via digital assent of a user agreement that is a prerequisite for transacting across the PayThat Payment System will legally bind them.

L.1.4: As noted on page 148 of the Proposal, “Compliance with various specific laws is discussed in detail: OFAC (page 25), BSA & AML (pages 14, 25, 32, 37, 39, 41, 42, 46, 73, 112, 114, 115, 117, 118), Regulation GG (page 25), Regulation E (pages 37-39, 41, 43, 46-48, 72), Regulation Z (page 48), MSB laws (page 25, 28, 32), all other applicable federal laws (page 50), all other applicable state laws (pages 49, 50).”

L.1.5: As noted on page 148 of the Proposal, “Because the PayThat Payment System only allows Depository Institutions to become PayThat Clearing Banks, and Depository Institutions are all subject to the same regulations with respect to electronic payments, there are no instances where Providers are performing the same functions, but are subject to different applicable laws. Any legal issues with respect to End-Users where there are instances where Providers are performing the same functions, but are subject to different applicable laws will be addressed in the Governance Documents (see page 50-51).” It is premature to build out or make additional decisions in that area of End-Users prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.2: Please provide more details regarding the Payment System Rules, including requirements, standards/protocols and procedures that govern the rights and obligations of all End Users, Providers, Payers and Payees. In doing so, please specifically address how the Solution supports the five Payment System Rules subcriteria.

L.2.1: As noted on page 148 of the Proposal, “Topics in the list are discussed as follows:
   L.2.1.1 Authentication of all Entities, payments or messages connected to a payment (see pages 24-34);
   L.2.1.2 Legal responsibility of Providers that provide Payment System access to End Users (see #1, #2, #3, #4, page 50);
   L.2.1.3 Payment Order Initiation/Authorization (see pages 29-36) and termination of Authorization (see page 35);
   L.2.1.4 Cancellation of a Payment (see page 35);
   L.2.1.5 Delayed and failed payments (see page 43, 47-50);
   L.2.1.6 Payment Finality (pages 41 and 36-39, 54, 55) and Settlement (see pages 43-44);
   L.2.1.7 Timing of sending and receipt of a payment (pages 38, 39, 41, 44);
   L.2.1.8 Records as proof of payment for Payers and Payees (see #4, page 50); and
   L.2.1.9 Error Resolution for anticipated disputed payments among End Users, Providers, Payers and Payees (see #4, page 50).”
L.2.2: As noted on page 148 of the Proposal, “The governance model, voting and amendment process by class of Entity and the process for obtaining input from PayThat Payment System stakeholders will be drafted within six months of the commencement of initial work to build PayThat (see #5, page 50).” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.2.3: As noted on page 149 of the Proposal, “The PayThat Payment System shall have the authority to examine and audit Entities and sanction and if necessary expel them from the PayThat Payment System (see #4, page 50).”

L.2.4: As noted on page 149 of the Proposal, “The allocation of losses due to the failure by the IAF, a Depository Institution or a PayThat Clearing Bank to properly vet End-Users during enrollment and authorization will be drafted within six months of the commencement of initial work to build PayThat (see #6, page 50).” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.2.5: As noted on page 149 of the Proposal, “Codification into specific written rules of the PayThat Payment System Rules regarding … the error resolution process … as described in this document will be drafted within six months of the commencement of initial work to build PayThat (see #4, page 50).” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.3: Please provide more details regarding consumer protections, including a Legal Framework and procedures that allocate legal and financial responsibility and support Error Resolution. In doing so, please specifically address how the Solution supports the three consumer protections subcriteria.

L.3.1: As noted on page 149 of the Proposal, “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 will be drafted within six months of the commencement of initial work to build PayThat (see #1, #2, #3, #4, #6 page 50). To the extent feasible the legal framework will follow Regulation E (pages 37-39, 41, 43, 46-48, 72) or Regulation Z (page 48), with respect to consumer rights, obligations and liability.”
This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.3.2: As noted on page 149 of the Proposal, “Payment System Rules and procedures that support Error Resolution for Consumer claims arising from payments Fraud, unauthorized payments or errors as described in this document will be drafted within six months of the commencement of initial work to build PayThat (see #1, #2, #3, #4, #6 page 50). To the extent feasible the legal framework will follow Regulation E (pages 37-39, 41, 43, 46-48, 72) or Regulation Z (page 48), with respect to consumer rights, obligations and liability.” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.3.3: As noted on page 149 of the Proposal, “Rules under which PayThat Clearing Banks or the PayThat Payment System itself may optionally establish for End Users and/or Providers additional Consumer protections for payments, which may exceed those protections that are otherwise required under applicable law will be drafted within six months of the commencement of initial work to build PayThat (see #7, page 50).” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

L.5: Please provide more details regarding intellectual property, including an approach to address any risks arising from third-party rights related to patents, trademarks, copyrights, and trade secrets. In doing so, please specifically address how the Solution supports the intellectual property subcriterion.

As noted on pages 150-151 of the Proposal, “Within six months of the commencement of initial work to build PayThat, an intellectual property search by a nationally recognized law firm specializing in intellectual property will be performed to determine a strategy to resolve or manage, prior to implementation, any legal, operational or financial risks to the Payment System, End Users and Providers arising from third-party intellectual property rights (including patents, trademarks, copyrights and trade secrets). To date, University Bank has only undertaken a partial due diligence investigation of potentially applicable intellectual property rights to the PayThat proposal, with the result that the patents listed in
this section have been identified. A significant amount of University Bank owned intellectual property has been incorporated into this copyrighted document (page 21).”

Prior to being granted two broad patents covering the PayThat Payment System, Jove Corporation, the owner of the patents engaged the Morgan Finnegan law firm, which at that time was the nation’s largest specialist intellectual property law firm, to discover any prior art. A significant sum of money was expended during this process. No relevant prior art was discovered and that is why the USPTO granted the patents. We would intend to use the Finnegan, Henderson, Farabow, Garrett & Dunner, LLP law firm, which is a nationally recognized intellectual property specialist law firm, to perform a search to determine if there is any risks arising from third-party rights related to patents, trademarks and copyrights. It would be very difficult to determine if there is any risk related to trade secrets, since by their nature, they are secret. PayThat Corporation will negotiate licensing agreements as needed using its cash resources. All of the entities mentioned in the proposal on pages 21-22 of the Proposal except for item #8 have informally committed to reasonable terms for licensing or purchasing the listed intellectual property. Because the PayThat Corporation will own all the required intellectual property or hold valid licenses covering all activities of the Payment System, End Users and Providers, it will be able to indemnify each of those entities related to any future assertions of intellectual property rights. If item #8 on page 22 of the Proposal cannot be licensed or purchased, that business (First Class Email) will not be able to be launched however that patent expires in not too many years, so this would be more of a delay than a permanent setback.

**Governance**

- G.1: Please provide more details regarding effective governance, including decision and rule-making processes that are transparent and support both the Solution's objectives and Public Policy Objectives. In doing so, please specifically address how the Solution supports the four effective governance subcriteria.

As noted on pages 152 of the Proposal, “Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The enumerated legal principles, rules and policies in G.1.1, G.1.2, G.1.3 and G.1.4 will be incorporated into these Governance Documents. (see page 50, #5).” This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

The Governance Documents will all be publicly disclosed on the PayThat Corporation website (G.1.2).

As noted on page 50 of the Proposal, the PayThat Payment System shall have the the authority to examine and audit Entities and sanction and if necessary expel them from the PayThat Payment System for material uncorrected failures to adhere to the network rules. This independent examination and audit process will provide independent validation of
compliance with the Solution’s rules, compliance with applicable law, and achievement of both the PayThat Payment System’s objectives and public policy objectives (G.1.4).

- G.2: Please provide more details regarding inclusive governance, including input and representation from diverse stakeholders, and support for the public interest. In doing so, please specifically address how the Solution supports the five inclusive governance subcriteria.

As noted on pages 152 of the Proposal, “Within six months of the commencement of initial work to build PayThat, a legal framework and governance agreement (the “Governance Documents”) will be created that binds all the Providers and End-Users of the PayThat Payment System. The enumerated legal principles, rules and policies in G.2.1, G.2.2, G.2.3, G.2.4 and G.2.5 will be incorporated into these Governance Documents. (see page 50, #5)”

This legal framework and governance agreement is likely to be modeled on the ECCHO Rules Model and we have received encouragement from ECCHO CEO David Walker in this regard. Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology. It is premature to build out or make additional decisions in this area prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.

The final Governance Documents shall include consideration of the public interest when making decisions and rules (G.2.1).

The final Governance Documents shall provide for input and influence by all stakeholders, through one or more governance or advisory bodies (G.2.2). One or more governance or advisory body shall be created.

The final Governance Documents shall have governance and advisory bodies that fairly represent stakeholders’ interests and risks (G.2.3). Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly inclusive methodology.

The final Governance Documents shall enable specific stakeholders or stakeholder groups to proportionately influence outcomes (G.2.4). Decisions required during the process of creating the Governance Documents will be made using the Federal Reserve Faster Payments Task Force Decision Marking Framework, which already meets this criterion.

The final Governance Documents shall address and manage actual, perceived, or potential conflicts of interest (G.2.5).

Again, in many of these areas, it is premature to build out or make additional decisions prior to engaging directly with the End Users and Providers including the PayThat Clearing Banks who will initially adopt PayThat.
Faster Payments QIAT

DRAFT ASSESSMENT
Faster Payments QIAT

DRAFT ASSESSMENT

Proposer: University Bank

Summary Description of Solution:

In a highly detailed proposal, University Bank describes PayThat, a closed-loop solution that provides good-funds transactions backed by funds held in a deposit account. PayThat is based on a system of end-user-controlled “cash purses” called PayThat CashBox, which is run by a network of networks (a set of licensed “Clearing Banks”) that interacts with but is separate from bank deposit, payment, and clearing systems. The PayThat system is built on top of, and interoperates with, existing legacy bank systems.

The solution is notable for its robust authentication of devices and individuals. It leverages email and SMS texting as ways to send and receive funds and their associated transaction data from a stored-value account (CashBox). Users’ accounts are prefunded to minimize risk through the transfer of funds from a traditional bank account. Funds are virtually present in the CashBox in the form of PayThat tokens, which are cryptographic artifacts that can be denominated in any currency (fiat or virtual). An identity management service called Identity Assurance Federation (IAF) maintains and encrypts users’ personally identifiable information (PII).

The solution depends on Clearing Banks that will process and react to PayThat messages, interact with PayThat databases, send and receive payments from the domestic legacy payment system, and interact with other Clearing Banks. Once money is in the CashBox, it remains there, allowing transactions within the solution to be settled within the closed loop. The proposal indicates that 12 Clearing Bank licenses will be sold: eight to banks in the U.S. and four to overseas banks. The solution thus depends on eight large U.S. financial institutions’ agreeing to act as Clearing Banks. International transactions will be supported through a Global Payment Gateway that has not yet been created. The proposer maintains that the solution can launch within 18 months.

EXECUTIVE SUMMARY OF THE PROPOSAL

- Major strengths
  - PayThat is a highly secure solution with strong authentication of both the device and the end-user. The solution includes an Identity Assurance Federation (IAF) that contains all PII and potentially other information as well. This information is fully encrypted with clearly designed and controlled access levels. End-users have the ability to determine who can have access to their information.
  
  - The proposal states that the PayThat solution is inexpensive for users to implement, operate, and maintain, and that it is less expensive to use than existing alternatives by at least 10x (p.11). The proposer claims that the solution can be built and rolled out to the market within 18 months, although it does need a partner to underwrite the initial platform development.

- Areas for improvement and enhancement
  - The solution relies on existing settlement capabilities (FedWire and ACH) and does not describe how a real-time clearing and settlement capability could be supported, if required. Settlement options vary within the solution. Individual transactions may be settled between Clearing Banks individually or in batch on a net settlement basis, account to account, or by using an existing legacy payment system such as ACH or FedWire.
– The solution’s viability depends on contracting eight to twelve large financial institutions (FIs) to act as Clearing Banks. The business case for FIs’ participation is unclear, yet the solution relies heavily on FIs’ abilities to address customer dissatisfaction, disputes, fraudulent transactions, Reg. E issues, etc.

– Given the level of authentication required at enrollment and beyond, the customer registration experience with PayThat could prove to be overly complex and may impact end-user adoption.

■ Use cases addressed

– The solution addresses all four major use cases (P2P, P2B, B2P, and B2B) and includes cross-border capabilities.

■ Proposer’s overall ability to deliver proposed solution

– The proposer’s ability to deliver the proposed solution hinges on their ability to enlist FIs to serve as Clearing Banks and to participate and support the initial platform build. Also key to the solution’s success will be the effectiveness of viral marketing techniques to drive end-user adoption.
ASSESSMENT

Ubiquity

U.1 Accessibility

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

**Rationale:**

The solution consists of a pre-funded account called CashBox. Funds can be loaded through payments received from registered PayThat users, through cash or check deposits made at merchant partner locations, or through transfers from a traditional deposit account. (It is not clear from the proposal whether the deposit account must be held at a Clearing Bank, or at a partner of a Clearing Bank.) The solution makes use of digital tokens that can be denominated in any currency.

PayThat allows users to load value from any type of account at any depository institution. Regulated non-bank account providers are not permitted to be PayThat Clearing Banks (p.45). Only licensed PayThat FIs can support clearing; they could therefore offer clearing services to non-licensed FIs.

Once the CashBox is funded, end-users can initiate payments to anyone using an email address, phone number or other supported alias. PayThat’s use of texting and email to send payments positions the solution to reach a significant portion of the “unbanked” population (U.1.4) as payees. If a payment is sent to a recipient who is not a PayThat user, the recipient will receive a marketing message inviting him/her to sign up for PayThat to access the funds. It is not clear from the proposal how recipients with deposit accounts at non-participating FIs will be able to access/withdraw their funds (U.1.1).

PayThat allows access to regulated non-bank account providers but requires those providers to hold funds in a master account at a depository institution (U.1.1, U.1.4). Moreover, funds cannot be deposited from CashBox into an account at a non-bank provider.

The solution supports cross-border payments and will also support multi-currency payments through its planned “Global Payment Gateway” (page 54) (U.1.3).

PayThat can only attain widespread adoption if it succeeds in signing on several large depository institutions as PayThat Clearing Banks (U.1.5-6). It is unclear how easy this task will be. The proposal can be strengthened by clearly describing how smaller FIs will participate as indirect connectors to PayThat.

The experience of end-users who hold an account in a non-Clearing Bank account should also be described. The end-user enrollment process requires substantial authentication steps, and it may have the unintended consequence of hampering adoption as a result.

PayThat has credible reach to end-users in that end-users can open accounts at PayThat Clearing Banks if their current FI is not a PayThat bank and they wish to participate. But the limited number of Clearing Banks may hinder adoption, and the attractiveness of PayThat participation to potential FI partners is uncertain. The solution is rated “Effective” here because partners must first sign on to bring the proposed use cases to life.
U.2 Usability

Very Effective    Effective    Somewhat Effective    Not Effective

Rationale:
PayThat is device-, channel-, and platform-agnostic (U.2.1). A payee need only have an email address or SMS-enabled mobile phone to send and receive a payment (U.2.2). The solution is accessible to the end-user 24x7x365; the only requirement is internet connectivity that persists through the transaction cycle (U.2.3).

The solution allows end-users to use their existing devices and any assistive methods associated with those devices. The UI (user interface) is simple, with few options, but end-users can access higher levels of complexity as desired. 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, assuming users are comfortable with their existing devices (U.2.4).

The solution is flexible enough to be integrated into existing merchant acquiring solutions or to be deployed as a separate work-around.

U.3 Predictability

Very Effective    Effective    Somewhat Effective    Not Effective

Rationale:
The core components of PayThat—the CashBox, PayThat Clearing Banks, eight messages, four databases, and the IAF’s enrollment and authentication services—deliver an end-user experience that is consistent across all channels (U.3.1, U.3.4). PayThat leverages email (SMTP) and text messaging (SMS) standards for communication at the end-user level (U.3.3). The error resolution process is predictable, as it is designed to address Regulation E and Regulation Z requirements (U.3.5). The solution is branded clearly as PayThat (U.3.6).

While the principles underpinning the operating rules are clear, it would be helpful to clarify whether the rules have been written and are in production (U.3.2) (p. 50).

U.4 Contextual data capability

Very Effective    Effective    Somewhat Effective    Not Effective

Rationale:
PayThat supports rich, XML-based, interoperable contextual data, as well as open APIs and help wizards to assist with interoperability and integration (U.4.1). The open API and help wizards automate the process of pulling data into standard industry business and personal finance systems (AP/AR, claims processing, payroll, treasury workstation, ERP systems, consumer accounting software, and tax reporting software) (U.4.2). The solution supports key industry standards for contextual data (e.g., STP820, ISO 20022, X12 data and UN CEFACT XML data), which is particularly important in helping to deliver the B2B use cases (U.4.3). XML data is captured and
shared using the “network of networks” architecture and APIs to standard ERP systems (e.g., Oracle, SAP, Microsoft, etc.).

The proposal can be bolstered by more clearly detailing how the various data formats could drive advancements in the payment system with respect to contextual data and its potential uses.

U.5 Cross-border functionality

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
A Global Payment Gateway—which has yet to be developed—is expected to facilitate a cross-border capability at implementation (U.5.1). The solution leverages ISO 20022 and UN CEFACT XML to support interoperability (U.5.2), and PayThat tokens can be denominated in any currency (U.5.4). PayThat Clearing Banks establish the solution’s exchange rates as an optional, value-added service. PayThat requires that all fees, rates, and terms be disclosed to the end-user prior to initiating a transaction, although it is left to the depository institution to provide the disclosure (U.5.3).

The proposal can benefit from articulating how the solution leverages the Gateway functionality to drive the acceptance of cross-border payments, and how the solution will be interoperable with other real-time payments systems around the world (U.5.2).

U.6 Applicability to multiple use cases

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
PayThat addresses the FPTF target use cases. Beyond that, the proposal outlines four use cases—with a detailed rationale for each—that go beyond traditional payments. The use cases are not considered to be within the scope of this evaluation, but they do provide examples of the extensibility of the PayThat solution.

Efficiency

E.1 Enables competition

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
PayThat will grant eight Clearing Licenses in the U.S. based on an RFP process designed to accelerate and drive adoption. One license will be held for a consortium of small FIs, a Bankers Bank, and/or a CUSO (credit union service organization) serving small FIs. Other non-licensed payment providers will be able to connect to PayThat through these Clearing Banks. It is not clear
how the limited Clearing Bank licenses may impact FI adoption. This design may result in end-users’ having a limited choice among PayThat account providers (E.1.1), and switching providers or using multiple providers may thus be challenging (E.1.2-3).

The solution’s interface and messaging content are specifically defined and may leave little room for providers to differentiate. However, the end-user-facing PayThat interface makes it easier for entities to use multiple providers. The proposal does state that participating banks are required to disclose pricing when users enroll in PayThat (E.1.3).

The proposal can be strengthened by clearly articulating how entities can easily switch between providers (E.1.3). It can further be enhanced by clarifying the incentives for banks to become Clearing Banks; the proposer does state that each license would be worth $3.5-$4.1 billion in three years with a 12.5% market share, but it would be helpful to describe the assumptions for how a Clearing Bank would attain such market share. Further, it would be beneficial to explain how an end-user can fund a CashBox if they do not have an account at a Clearing Bank or at an FI that is associated with a Clearing Bank via a correspondent banking relationship.

### E.2 Capability to enable value-added services

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

**Rationale:**

PayThat supports the transmission and use of rich, XML-based, interoperable contextual data which can be leveraged to introduce additional services. PayThat also provides open, published APIs and help wizards that should allow payment service providers of all sizes to develop and provide value-added services, particularly data-driven offerings (E.2.1-2). PayThat’s operating rules require FIs to fully disclose any fees, etc. before fees are incurred, making the value proposition easily understandable to all end-users (E.1.3).

### E.3 Implementation timeline

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

**Rationale:**

The proposal indicates that building the PayThat Clearing Bank software solution should take approximately six months. Integration timeline estimates are not provided. The four databases contained in the solution can be built and tested in parallel and should also be completed in six months. To support cross-border payments, a Global Payments Gateway solution must be defined. The proposal suggests leveraging an existing global payment gateway operated by one of the major global banks (which would take one to three months) or building a GPG in partnership with a major global bank (six to twelve months). The total timeline seems to be about 12 months, with system operability and ubiquity increasing over the ensuing 18 months.

The solution requires eight large banks to agree to act as PayThat Clearing Banks. The Proposal would benefit from a clear articulation of the “initial” incentives for a bank to join PayThat as a Clearing Bank. The proposal assumes that existing bank operations/capabilities will be leveraged for customer complaints and fraud management. This assumption will need to be validated.
The proposal suggests an 18-month launch for PayThat but requires a partner to fund the building of the platform. The proposal indicates that funding should be readily available from the FinTech/venture capital community, or Depository Institutions could fund the cost of the solution themselves. (Total cost is anticipated to be less than $10MM.)

End-user growth relies heavily on a viral marketing approach based on enrollment by recipients of payments from PayThat users: to claim a payment, the recipient must enroll in PayThat. The lengthy, complex enrollment process and the limited number of Clearing Banks may hinder adoption.

E.4 Payment format standards

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
PayThat supports several key industry standards: STP820, ISO 20022, X12 and UN CEFACT XML (E.4.1). These formats enable cross-border interoperability (E.4.2), are cost-effective to adopt (E.4.3), are adaptable, and facilitate innovation (E.4.4).

E.5 Comprehensive

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
In concert with FIs, which are responsible for various aspects of the end-to-end payment process, PayThat is able to deliver an end-to-end payment process from initiation to reconciliation (E.5.1). The Solution’s technical design supports all of its features (E.5.2). For transactions involving the conversion of PayThat tokens to fiat currency, the solution does not directly settle transactions but rather relies on Clearing Banks to use existing settlement mechanisms to determine settlement rules and windows between themselves (E.5.1-2).

E.6 Scalability and adaptability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
PayThat is expected to support the projected use cases (E.6.1), and the proposal asserts that the solution’s technical design is adaptable and flexible (E.6.2). It describes a “network-of-networks” architecture, but it would be helpful to provide more details about the hardware and software required to support the solution. The system’s messaging is based on SMTP and SMS standards, which have proven to be capable of handling millions of transactions per second and scale well. The proposal also states that “SWIFTNet runs an XML-compatible payment system with high transaction volumes without difficulty at comparable transaction levels to what VISANet handles [sic]” (page 132). The solution will be “stress-tested” quarterly at transaction rates 20x higher than historic peak volume.
The proposal can be strengthened by a technical explanation of how the system will scale (E.6.2). Additionally, providing insight into how the solution would adapt to future changes and needs in the payments system would be helpful to the proposal’s overall value proposition (E.6.3).

### E.7 Exceptions and investigations process

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

**Rationale:**

The solution relies on the PayThat Clearing Banks’ existing tools and protocols for exceptions and investigations to address customer complaints, fraud reports, and Regulation E issues (E.7.1-2). Because PayThat is available 24x7x365, Clearing Banks will have to expand their exceptions and investigations process to become 24x7x365 as well. This requirement may present an implementation challenge.

Transaction-related information is stored in PayThat servers and databases for seven years. This information is expected to be available to Clearing Banks to address and resolve disputes. The proposal does not provide any tools to Clearing Banks for dispute resolution. The proposal could be enhanced by describing any available capability for Clearing Banks to search these databases for exception-related information.

The Identity Assurance Federation (IAF) is responsible for managing the fraud detection system (p.137); however, the relationship between PayThat and the IAF is unclear. The IAF is not part of the network diagram on page 47 of the proposal. The proposal can be strengthened by articulating whether fraud monitoring occurs in real time or batch and explaining how information from PayThat servers is accessible to the IAF for monitoring. It would be helpful to explain in detail how PayThat and IAF work in conjunction to manage and monitor fraud - including detecting patterns at the individual or aggregate level (E.7.2).

### 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:**

As designed, PayThat relies on robust end-user authentication, pre-funded accounts to support push payments, and blocked funds to support multiple settlement models. As designed, the risk management framework to be applied to the solution is thorough. The solution relies on pre-funded end-user accounts (S.1.2) to mitigate risk and on end users to identify fraudulent transactions (S.1.4). However, the rules for risk management have yet to be written (although it is clearly stated that rules will be written within six months of the platform build).

The proposal could be strengthened by addressing the incentives for operators and providers to manage the risk that they could pose to other participants (S.1.5), as well as by describing how the risk management framework will be periodically reviewed and updated while in production (S.1.6).
S.2 Payer authorization

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**

Payers can pre-authorize payments under certain parameters (S.2.2), revoke those payments in real time, or change payment parameters in real time (S.2.3). To promote safety and soundness, the solution requires authentication of both the device and the consumer (S.2.1). There are slight concerns that consumer authentication at Levels 3 and 4 (i.e., authentication of both device and consumer) may discourage usage and/or enrollment and thereby inhibit overall deployment.

S.3 Payment finality

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**

To ensure a “good-funds” model, the solution requires the Clearing Bank to validate the CashBox balance prior to initiating a transaction (S3.1). Funds are available to the recipient as soon as the receiving FI accepts the payment. Given its use of pre-funded accounts, the solution meets the requirement that FIs or non-bank providers be compelled to approve payments after their initiation to assure the availability of good funds in the payer’s account (S.1.1). The payment becomes final and legally irrevocable once Regulation E’s time provisions have expired (S.3.2). Same-day ACH and the introduction of real-time payment networks are expected to expedite the payment’s finality.

The proposal could be improved by discussing the mechanisms and processes—beyond the Clearing Bank’s existing processes for dispute resolution—to protect or compensate the payer in the event of a dispute (S.3.3).

S.4 Settlement approach

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**

PayThat holds stored value inside a PayThat account. This good-funds model essentially eliminates risk for all “in-system” transactions. The stored value is backed by good funds held within dedicated bank accounts that can only be credited or debited by the depository institution that holds the bank account. The dedicated bank accounts represent the activities of the CashBox accounts that are linked to them and support settlement in central bank money (S.4.3). The proposal assumes that the depository institutions would settle with the Clearing Banks periodically, based on accumulated balances owing or a time window. The proposal states that typical settlement would occur within 30 minutes or less (S.4.1). Settlement for transactions that move funds in and out of CashBox accounts may occur via ACH or FedWire, and amounts may or may not be net. Because PayThat is available 24x7x365, and current settlement capabilities are not, Clearing Banks will be required to hold sufficient good funds in central bank money escrow accounts to cover settlement obligations and to address settlement risk when clearing facilities are not operating (i.e., overnight, on weekends, and on holidays) (S4.2). The solution requires Clearing Banks to settle using a pre-
funded account or an approved credit line, which should eliminate the risk associated with imbalances in the payments system.

S.5 Handling disputed payments

Very Effective       Effective        Somewhat Effective       Not Effective

Rationale:
The solution relies on existing FI processes to handle customer complaints, fraud reports, and Regulation E and Z issues. How these existing processes may need to be modified within participating FIs to accommodate PayThat accounts is unclear. The data stored in the solution’s four databases may be accessed via credentials differentiated by role, authority, authenticated status, and a “need to know.”

The proposal can be strengthened by outlining a minimum set of requirements for banks to follow in handling disputes of unauthorized transactions (S.5.1). There are concerns that a court proceeding may not be an effective way to handle disputed payments (e.g., handling them via operating rules may be preferable).

S.6 Fraud information sharing

Very Effective       Effective        Somewhat Effective       Not Effective

Rationale:
The proposal states that the IAF will facilitate timely, frequent information-sharing among all providers, operators, and regulators to assist in the management, monitoring, and mitigation of fraud and evolving threats in accordance with applicable law (S.6.3). Moreover, PayThat payment rules will require the sharing of information to support the management and monitoring of fraud (S.6.1). PayThat captures transaction information, aggregates it in the IAF, and permissions access (S.6.6).

The proposal describes in detail how data owned by entities other than providers or operators would be aggregated, managed, and protected (S.6.2) (page 137). The solution’s information-sharing mechanisms are easy to implement, update, and maintain, and they support differentiated access to content (S.6.4-5). The IAF is intended to manage fraud detection, which includes identifying patterns at the individual or aggregate level (S.6.7). The proposal does not define how patterns will be identified, however.

The Proposal can be enhanced by discussing the logic by which the IAF will monitor transactions and identify suspicious transaction patterns (S.6.3 and S.6.7). Additionally, the proposal would benefit from articulating the type of payment data that is available to be viewed (S.6.1).
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 proposal indicates that the PayThat solution will include strong technical access components and controls, which are alluded to in the proposal (S.7.1) (pp. 137-138), but can be strengthened by providing details as to how these requirements will be met. For example, the proposal states that the PayThat databases will be physically housed in enterprise-network-server data centers that are compliant with FFIEC standards, but it does not indicate where these data centers will be located (e.g., geographically dispersed locations) or the measures that will be taken to meet FFIEC standards. It does provide detailed documentation of operational and procedural controls (S.7.2) (page 138). The proposal can be further enhanced by providing details of a framework that will guide the composition of the solution’s managerial policies and oversight plans (S.7.3).

S.8 Resiliency

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

**Rationale:**

The proposal describes a system that will deliver FFIEC-compliant policies and procedures for disaster recovery and business resiliency, but can be made more robust by detailing the policies and procedures (S.8.2-4). The solution will incorporate FFIEC requirements pertaining to Sigma 6 uptime (S.8.1) by ensuring critical path systems will be geographically dispersed with immediate failover capability. The solution will maintain different schedules—ranging from daily to annual—for specific tasks associated with resiliency testing (S.8.5).

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 requires that all data in motion and at rest be encrypted (S.9.1). PayThat is designed to ensure that end-users do not need to know each other’s account numbers to initiate or receive payments. Once an end-user has been “strongly enrolled,” no PII will be required to authenticate transactions (S.9.2-3). The proposal states that the PayThat Payment System’s four databases will store all data for seven years (or less if required by applicable laws and regulation). Monitoring and malicious-pattern-detection systems will protect all nodes in the system by monitoring for data breaches. (These systems will be selected following an RFP.) PayThat will require all data to be encrypted in motion or at rest, and access will be provided on a need-to-know basis based on role, authority, and authentication status (S.9.2-3). The proposer specifically states that “ASC-X9 Encryption Standards will be used to encrypt end-user data using methods known as Digital Rights Management (DRM).”
The proposal could be improved by explaining how access to the solution’s databases will be supported, managed, or monitored (S.9.2-3).

## S.10 End-user/provider authentication

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

**Rationale:**

The PayThat solution will use the NIST 800-63-2 standard for enrollment and ongoing authentication of users and providers. (The NIST standard provides technical guidelines for Federal agencies’ digital authentication of users who interact with government IT systems over open networks. These guidelines address only traditional, widely implemented methods for digital authentication, based on secrets [per NIST website]. The standard has recently been replaced by 800-63-3.) The solution also aligns with FFIEC guidance and standards for authentication (S.10.1, S.10.3).

Per NIST, the level of identity-proofing assurance will rise from Level 1 to Level 4 based on the risk and dollar size of the proposed transaction. The solution supports robust authentication based on physical/biometric traits coupled with a personal possession that has been strongly enrolled and authenticated. The proposal indicates that the sender chooses the authentication method and can use any security method that is supported by the solution.

## 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:**

Providers must agree and adhere to rules via a participation agreement, but these rules have not yet been built. The proposal clearly states that the rules will be written within six months of commencing the initial build of the PayThat platform.

**Speed (Fast)**

## F.1 Fast approval

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

**Rationale:**

The transmission and receipt of the solution’s eight payment messages should take less than two seconds, thereby meeting and exceeding the goals of the Faster Payments Effectiveness Criteria.
F.2 Fast clearing

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

**Rationale:**
The transmission and receipt of the solution’s eight payment messages should take less than two seconds, thereby meeting and exceeding the goals of the Faster Payments Effectiveness Criteria.

F.3 Fast availability of good funds to payee

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

**Rationale:**
The transmission and receipt of the solution’s eight payment messages should take less than two seconds. Authentication to the CashBox should take less than 30 seconds. The payee should then have immediate access to the PayThat tokens in the .pay file and to any contextual data the payee has rights to, based on the privacy template, authority, need to know, and authenticated status.

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

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

**Rationale**
PayThat Clearing Banks settle in real-time, but can agree amongst themselves to other methods, such as: (1) on a net basis periodically throughout the day when the accumulated amount owed exceeds $200,000; or (2) at intervals not to exceed 30 minutes as agreed between participating Clearing Banks (F.4.3). Correspondent banks of the Clearing Banks would provide cash balances or lines of credit to support these settlement options. No funds are ever required to be transmitted or settled via traditional bank payment systems (ACH, FedWire etc.).

The PayThat network is available 24x7x365. A detailed approach to managing credit and liquidity risk exposures is not described (F.4.1). To ensure that accounts at Clearing Banks can be funded even when legacy systems are not available (e.g., on holidays and non-business days), system rules will require good funds to be held in central bank money escrow accounts. That way, funds will be available to cover the net settlement risk among PayThat clearing banks and the correspondent banks of the PayThat Clearing Banks (F.4.2).

F.5 Prompt visibility of payment status

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

**Rationale:**
As described, the solution sends notifications of payments to the payer’s CashBox (F.5.1). When a payment is made, the payee receives a notification via email or text. The payment’s status is immediately visible to the payer as a pending, authorized transaction in the participant's CashBox.
(F.5.2). Once the payment has been accepted, the remaining notifications are available within CashBox as well.

The proposal can be enhanced by clearly articulating whether the end user receives the notifications via a push mechanism or the must be logged into CashBox to be aware of them.

**Legal**

**L.1  Legal framework**

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

**Rationale:**

PayThat’s rules and legal framework have not yet been established, but the proposal describes a clear, thorough plan for building out the legal framework within six months of commencing to build PayThat. No existing rules or laws need to be changed to accommodate PayThat, as the solution will be designed to operate within the legal boundaries of the current payment system (L.1.2). The proposal cites no instances wherein end-users would perform the same functions in the payment system but would be subject to different banking and payment laws. All providers (Clearing Banks) must be FIs and therefore are all subject to the same applicable laws (L.1.5). The PayThat System Governance Documents will define requirements where there is no definitive legal guidance currently in place.

The proposal acknowledges a need for a legal framework and sets out a path to develop it (e.g., the legal framework is likely to be modeled on the ECCHO Rules Model), but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

**L.2  Payment system rules**

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

**Rationale:**

As with the legal framework, the payment system rules for PayThat have not yet been written. According to the proposal, the rules will be drafted within six months after commencing work on building the solution. The proposal does discuss several key aspects of these rules, such as the fact that the PayThat system will have the authority to examine, audit, and—if necessary—sanction entities (L.2.3).

The proposal can be strengthened by describing a process for amending the rules (L.2.2) and for resolving errors (L.2.5). The proposer should ensure that these processes are addressed in the initial draft of the rules.

The proposal acknowledges a need for payment system rules and sets out a path to complete them (e.g., the legal framework is likely to be modeled on the ECCHO Rules Model), but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
L.3 Consumer protections

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**

Consumer protections are not defined in the proposal, as the legal framework has not yet been written. The legal framework and payment system rules to support error resolution will be drafted within six months of commencement of initial work to build PayThat. The proposal does discuss several key aspects of the system’s rules, and Regulation E and Regulation Z are specifically mentioned. To the extent feasible the legal framework will follow Regulation E and Regulation Z. It will be possible for Clearing Banks or the PayThat system to optionally establish additional consumer protections that exceed those required under applicable law.

The proposal acknowledges a need for consumer protections and sets out a path to complete them (e.g., the legal framework is likely to be modeled on the ECCHO Rules Model), but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective”

L.4 Data privacy

**Very Effective**

**Rationale:**

PayThat and its developers have set forth a detailed, effective approach to data privacy, confidentiality, and security of payment and related data that includes user-controlled access and standard privacy templates (pp. 149-151). At enrollment, participants select a privacy template level that can be fine-tuned to the specific needs of an end-user or industry vertical (e.g., healthcare for HIPAA requirements). The .pay files uses cryptographic standards so that each data element is separately encrypted and accessible solely based on role, authority, authentication status, and “need to know.”

L.5 Intellectual property

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**

Within six months of commencement of initial work to build PayThat, an intellectual property search will be performed. To date, a due diligence investigation has only been partially completed, with identified patents listed in the proposal (pp. 21-22).
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 proposer has not yet written governance documents for PayThat but will write them within six months of commencing to build PayThat. Based on the rules and policies outlined in sections G1-G4 and G2-G4 of the proposal, all required aspects of effective governance are expected to be incorporated into the governance documents.

The governance agreement is likely to be modeled on the ECCHO Rule Model. Decisions required during the development of the governance model will be made using the Federal Reserve Faster Payments Task Force’s decision-making framework.

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

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 proposer has not yet written governance documents for PayThat but will write them within six months of commencing to build PayThat (e.g., the governance framework is likely to be modeled on the ECCHO Rules Model).

The proposal describes key attributes of the proposed governance framework, acknowledges a need for inclusive governance, and sets out a path to develop such a framework, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
# APPENDIX A: ASSESSMENT SUMMARY

- ✓ = QIAT Assessment
- ○ = Proposer Self-Assessment

## UBIQUITY

<table>
<thead>
<tr>
<th>UBIQUITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.1: Accessibility</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2: Usability</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.3: Predictability</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.4: Contextual data capability</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.5: Cross-border functionality</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.6: Multiple use case applicability</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## EFFICIENCY

<table>
<thead>
<tr>
<th>EFFICIENCY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1: Enables competition</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2: Capability to add value-added services</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.3: Implementation timeline</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.4: Payment format standards</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.5: Comprehensive</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.6: Scalability and adaptability</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.7: Exceptions and investigations process</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## SAFETY AND SECURITY

<table>
<thead>
<tr>
<th>SAFETY AND SECURITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td>✓ ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAFETY AND SECURITY (cont’d)</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>-------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPEED (FAST)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.1: Fast approval</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGAL</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1: Legal framework</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td>✓○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1: Effective governance</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

PayThat Has a Superior Business Model and Adoption Path

Using the four innovative adoption use cases detailed in the Proposal (see pages 75-123), the entire PayThat Network would be worth $29.58 billion to $34.35 billion. Between one and eight FIs can obtain a license to own, build and deploy a PayThat node, called a PayThat Clearing Bank. If only one large or medium sized FI adopts PayThat and obtains 100% market share of the four use cases detailed in the proposal, the value of its PayThat Clearing Bank would be $28.64 billion to $32.8 billion. If the maximum number of eight FIs purchase licenses and deploys a PayThat Clearing Bank and split the market share for PayThat services equally, for a modest investment to purchase a license, they would own a fee driven business that for each of the eight licensees would be worth $3.58 billion to $4.1 billion within three years if they achieve that average market share of 12.5%. The PayThat Corporation itself would be worth $940 million to $1.55 billion (see page 104 of the Proposal). One to four additional overseas FI licenses would be available that would generate significant additional value.

The key problem with any new U.S. payment system proposal is achieving adoption. We have outlined four niche adoption use cases that are compelling:

− Use Case #1 is worth at least $1 billion for the PayThat enabled Health Information Exchange payment system proposal as the PayThat HIE services will capture a portion of the $4.5 billion off administrative costs for doctors and hospitals, private health plans, states and other government health plans that HHS has estimated can be saved by adoption of such a system over the next 10 years (see pages 75 & 79 of the Proposal).

− Use Case #2 Each PayThat Clearing Bank would own a fee driven business that would have a value of between $780 million and $1.30 billion at the end of the third year after the launch of the First Class Email product (see page 106 of the Proposal).

− Use Case #3 is worth at least $1 billion for the Single Window for Cross Border Trade Facilitation & Supply Chain Billing (see pages 108-112 of the Proposal).

− Use Case #4 is worth $10.2 billion for the credit bureau alone and likely at least double that for the IAF (see page 114 of the Proposal).

Since the PayThat Corporation would be worth $940 million to $1.55 billion (see page 104 of the Proposal), and potentially more as international business grows, and because the cost to build the four use cases targeted by the PayThat Payment System is under $100 million, this is an attractive venture capital opportunity.

PayThat’s Technical Design Using “Network of Networks” & “Data Centric Encryption”

PayThat uses a superior “Data-Centric” approach to encryption and a “network of networks” architectural approach leveraging XML and XML tagged data pushed to edge servers from legacy applications, extending the usefulness of legacy applications and dramatically lowering cost of adoption for innovative solutions. The architecture methods of PayThat enable the following positive attributes as opposed to the negative attributes of the legacy payment systems and other emerging innovative solutions now deployed in the United States (see page 10 of the Proposal):
Because PayThat uses a “network of networks” architectural approach leveraging:

- XML
- XML tagged data pushed to edge servers from legacy applications
- Mapping; and
- Interoperability standards
- Edge Servers
- a “Data-Centric” approach to encryption

interoperability among legacy infrastructures such as legacy bank platforms and bank payment systems can be ensured, extending their usefulness and dramatically lowering cost of adoption for innovative solutions. The points of integration are greatly reduced and legacy systems are unaffected in their daily operation. See pages 120 to 123 for a more detailed description of the “network of network” architecture and methods of implementation.

In the PayThat use cases, the only points of integration are between the PayThat Clearing Banks, which serve as “edge servers” for traditional Depository Institutions and the payment systems of those traditional Depository Institutions. The integration required is equivalent to a banking corporate treasury workstation. The integration is modest and should only take weeks. By design and purposefully the amount of IT integration with the systems of legacy Depository Institutions is kept to a minimal level. Since most corporate treasury workstation solutions support data exporting and data importing, the challenge is mostly reduced to mapping and by using state of the art mapping automation tools, which have low six figure costs, the technical challenge is low and the technical risk is low.

Creating XML tagged databases is also a task where the technical challenge is low and the technical risk is low. Where any of the use cases require interaction with any pre-existing legacy solution, the same architectural approach and means of integrating and creating a means of enabling data interoperability with be used: data will be pushed to edge servers from legacy applications, where the data is XML tagged by individual data element and encrypted with Persistent Digital Security (a/k/a Digital Rights Management).

By using a “Data-Centric” approach to encryption where data access is controlled by role & authority on a transaction level basis, access to all data is controlled by users at the network nodes where the edge servers reside with access controlled by rules enforced by strong encryption, providing greater control & security. This technical solution greatly enhances personal privacy and if and when PayThat achieves market dominance, it will destroy the economics of the identity theft criminal ecosystem.

Among PayThat’s technical advisors is Ed Scheidt, the Chief Scientist and Co-Founder of TecSec, who is also the retired Chairman of the Central Intelligence Agency (CIA) Cryptographic Center and the Chair person for ASC X9F, which develops the cryptographic standards for the U.S. financial services industry.

The “network of network” technical design has been successfully deployed for 10x to 100x lower cost than traditional “single network/single solution/single database” (SSS) solutions. SSS technical solutions also carry a high probability of project failure, while “network of network” solutions such as PayThat have low technical risk.
The Global Payment Gateway:
The Global Payment Gateway (GPG) is a web service built by Depository Institutions that communicates through and leverages legacy payment networks in each country around the world to enable cross-border payment functionality in real-time leveraging RTGS and ACH payment systems around the world. The concept was first piloted in the Universal Value eXchange (UVX) pilot of the Financial Services Technology Consortium (FSTC). Several major banks have since built GPGs including Wells Fargo and Chase Bank. The PayThat Payment System would either utilize one or more of the existing GPGs selected by RFP, or build a new one in partnership with a large bank selected via RFP. Building a GPG is a low-risk project. See pages 54-57 of the Proposal.

Achieving Strong Enrollment & Strong Authentication While Achieving Rapid Adoption
We have designed robust security, enrollment and authentication of users of PayThat. However, we have built in best practice to achieve strong enrollment and strong authentication without discouraging adoption. The key to achieving this balance is to start at a commercially reasonable initial lower level of enrollment and authentication and then require customers to jump over additional hurdles when they wish to perform a transaction that poses more risk that the risk model allows prior to increasing the assurance of identity and authentication status. Customers have a high willingness to comply with additional requirements if they have a pending transaction that they wish to complete. As noted on pages 25 & 32-33 of the proposal:

“End-users will be required to jump though additional incremental enrollment barriers as they wish to do progressively larger and/or more risky transactions (e.g. red flag industries, such as a transaction with a Money Services Business (MSB) vendor or higher risk transaction types, for example purchasing wine where a minimum age requirement must be met, and international transfers, or prohibited transactions, such as a gambling transaction prohibited by Regulation GG). Improvements in the degree to which identity is proofed should be multi-faceted and incremental with no single solution or step which is final. Some devices are inherently more secure than others and therefore the devices will be risk-rated and escalation of security methods will occur more rapidly with less secure devices.”

Secure Internet Payments: What is needed?
- Intuitive and easy to use & adopt
- Something as easy as email
- Platform/device independent & agnostic:
- Secure way to send money over insecure email & telecommunication networks
- Greatly enhanced consumer privacy and the elimination of the identity theft ecosystem.

PayThat and the Identity Assurance Federation, a federated identity management service, can achieve all these requirements.

Adoption is the key. What will be the successful adoption use cases that actually gain mass market acceptance of a new, more secure payment system and identity management system?

We have developed six detailed use cases and business models, each of which is large enough to move the needle at even a large financial institution. Four use cases were detailed in the proposal at length. A high level summary of each use case follows:
First Class Email Use Case

- 20% or more of Bank Employees typically click on malicious email links.
- If the CryptoLocker virus is combined with the Stuxnet worm and a time delayed payload bomb to corrupt data stored in backup files, no U.S. bank would survive because of the length of time required to restore from a good backup not impacted.
- The use of wild email will be unsafe and unsound for banks and business in the near future.
- PayThat will move the banking industry away from wild email to “First Class Email”.
- Under “First Class Email”, no unauthenticated email will be presented to email users. All malicious spam will be blocked at the “First Class Email” Simple Mail Transfer Protocol (SMTP) gateway.
- PayThat network rules will create a protected zone of the internet, where only authenticated users can send or receive email and where senders of all email must attach a valid, good funds, immediately negotiable electronic check in the form of a PayThat Token in the amount of at least one U.S. cent.
- By substantially raising the cost of spam, the economics of the hacker gangs will be fatally undermined. As a major side benefit, the productivity of corporate workers will rise substantially as unwanted spam is eliminated from their daily routine and they will actually earn money to receive and read any unwanted “First Class Email”.

Healthcare Payments Use Case

- The healthcare sector is the largest single industry in the U.S., contributing 17.6% of the nation’s GDP, however it has the lowest adoption of electronic payments with 95% of healthcare related payments ending up ultimately as a paper check.
- Administrative overhead is high at 30% of overall costs because healthcare claims data (held by healthcare insurance firms, FIs and healthcare providers) and healthcare clinical data (held by healthcare providers) are siloed in separate business processes and reconciliation between the two silos is time consuming and expensive. Consumers receive healthcare bills & Explanation of Benefits (EOBs) that are not synchronized and frequently contain non-reconciled differences.
- Healthcare providers, because they typically only rely on user name and password to access HIPAA controlled PII and have rarely deployed encryption to protect their data, have experienced rapidly rising security breaches.
- More secure identity management systems combined with health information exchange services using a “network of networks” & “data centric” data encryption approach and payment automation offer the prospect of greater security, enhanced privacy and over $4.5 billion in cost savings just from the widespread adoption of electronic payments. A portion of those savings will accrue to the FI service providers.
- PayThat’s Payment System and PayThat’s Identity Assurance Federation (IAF) can achieve these efficiencies.
Starting with a pilot implementation in Michigan covering 1.5% of the population the U.S., PayThat’s healthcare payments automation services will be adopted by other health information exchanges nationwide and ultimately roll out to the entire U.S. population and to mass merchants through their retail pharmacy operations.

Cross Border Trade Use Case

- To import or export goods into or out of the United States, signed documents must be procured from 33 different federal government agencies. This is an expensive, complicated and time-consuming paper intensive process. Most smaller manufacturing firms based in the U.S. are discouraged by these barriers from exporting.

- The Single Window allows a firm that wants to export or import any goods across the borders of the U.S. the ability to obtain all the documents required by filling out just one intelligent web form. At the end of the process, the End-User digitally signs the intelligent web form once and all the required information, certificates and documents are prepared behind the scenes in an automated fashion by the various government bodies. Certificates and documents are created in real-time on-line and delivered in a secure electronic portal to the End-User by accessing the databases of the applicable government agencies. The interoperability with the legacy government agency applications would be accomplished using “edge servers” and the “network of networks” technical design.

- President Obama signed an executive order in February 2014 directing the federal government to establish a “Single Window” to facilitate cross-border trade by December 2016. This is a large effort across 43 federal government agencies. However, to date, the federal government effort to implement the Single Window is not focused on any business use cases or adoption strategies and has little functionality.

- Detroit, Michigan, home of the U.S. auto industry and site of the largest customs port of entry, is a natural candidate for a “Single Window” pilot focused on the automotive supply chain.

- The Single Window earns fees for the basic service and from value added services offered through the Single Window to End-Users. PayThat’s Payment System and PayThat’s Identity Assurance Federation (IAF) is a critical component to achieving these revenues & efficiencies.

Identity Assurance Federation & Credit Bureau Use Case

- There is no trustworthy web service that can strongly enroll and authenticate to NIST Level 3 or 4 consumers or business employees to enable sufficiently strong cyber security to safely engage in e-commerce.

- To comply with Anti-Money Laundering (AML), Bank Secrecy Act (BSA) and the new Foreign Account Tax Compliance Act (FATCA) laws, each bank is now required to know and identify their customers, understand the business of each customer and understand the transactions flowing through their customers’ deposit accounts to non-customers. To actually and fully comply with these requirements is a near impossibility if the regulations are strictly applied, however, non-compliance carries with it the possibility of massive multi-billion dollar fines and severe reputation risk. The cost for
each bank to individually do this work is far more costly and carries much greater compliance risk than if the work were outsourced to an industry back office utility, a bank owned Identity Assurance Federation (IAF).

- The IAF service will validate identities and perform identity management. The IAF can provide these services at much lower cost than any Depository Institution or any other party.
- Because the IAF builds a database of attributes related to individual and corporate participants and End-Users, the IAF can append additional data about these participants and End-Users at low cost. The appended data can be used to build a Depository Institution owned Credit Bureau and a Depository Institution owned B2B Directory. The value of the U.S. credit bureau industry, currently owned by non-banks, is $17 billion. Because much of the valuable data resident in the existing credit bureaus is supplied to them for free by FIs, the IAF’s credit bureau should be able to achieve a 60% market share of the U.S. credit bureau industry, creating $10.2 billion in value for the owners of the IAF.

Unbanked Use Case

- Why Don’t Banks Seek Low-Balance Deposit Accounts? Using traditional methods, low balance accounts lose money.
- To be profitable a bank account must have:
  - Average deposits of $600 to offset paper statement costs:
    - $0.50 per month x 12 = $6 per year. If cost of funds is 1%
      ($6/.01=6x100=$600);
    - Incur overdrafts or other fees to offset cost of teller services:
      - Teller transactions cost $2 each on average;
      - Branch system brick and mortar is costly.
- With internet/mobile phone based deposit accounts serviced remotely, ALL accounts with balances can be profitable:
  - If customers require any unusual service needs they pay by the minute used via 900# customer service;
  - 100% electronic access allows the overhead associated with an additional account to be very close to zero.
- Mobile Phone Based Banking: What is needed?
  - Intuitive and easy to use & adopt, “Something as easy as email”;
  - +90% of Internet users use email;
  - Something that uses either email or text message:
    - In U.S. the average number of monthly:
      - Phone calls = 204;
      - Text messages = 357;
  - Platform/device independent & agnostic: PC, Mobile Device, Any Platform;
  - Secure way to send money over insecure networks.
- PayThat & the IAF together achieve each requirement. Its design was the model for India’s new national payment system and biometric IdM system, with 600 million new users within the first year. Most of them had never been banked before.

Replacement for SWIFT Use Case

- SWIFT, the current main cross-border payment system uses an insecure network node design methodology and has suffered a series of major breaches.
- SWIFT is a messaging system only, and does not perform settlement or clearing. Outside of the OECD countries, it often takes one or two weeks to get international transactions settled and cleared. There is no visibility of the status of a payment until it arrives and multiple banks can often be involved in a single transaction.
- PayThat could serve as a SWIFT replacement focusing on small businesses that do business in two or more countries in the developing world.
- The IAF would provide strong enrollment including Know Your Customer due diligence.
- A Global Payment Gateway would enable same day settlement in every national payment system around the world.
- Banks would find it useful as international wires are a major regulatory risk and service quality is low.
- Once the system is built for this use case it can easily be extended into additional use cases including the five outlined above.
- If SWIFT doesn't replace its system architecture with a more secure PayThat equivalent, PayThat might ultimately replace SWIFT by taking its customers away.

The following statements in the McKinsey Draft Assessment are inaccurate:

Page 1: “The solution relies on existing settlement capabilities (FedWire and ACH) and does not describe how a real-time clearing and settlement capability could be supported, if required.” McKinsey’s own evaluation states on page 1 “Once money is in the CashBox, it remains there, allowing transactions within the solution to be settled within the closed loop,” and rates criterion S.4 Settlement Approach as “Highly Effective”. Only if two PayThat Clearing Banks use a different depository to hold their escrowed funds and only if a net amount of good funds shifts between two PayThat Clearing Banks is a settlement in legacy funds required. That preferred method of FIs for inter-FI settlement is currently Wire (either FedWire or Clearing House Wire) or ACH, however any legacy or future settlement method could be supported and the PayThat Solution does not “rely” on this, except in a tangential manner as some method of settling net differences that arise must be used if there is more than one PayThat Clearing Bank. If there is only one PayThat Clearing Bank the issue disappears completely.

Page 2: “The solution’s viability depends on contracting eight to twelve large financial institutions (FIs) to act as Clearing Banks. The business case for FIs’ participation is unclear...” Only one medium or large FI is required to successfully launch the system. We place a limit of 8
domestic and 4 international licenses for PayThat Clearing Banks to encourage early adoption and discourage late adoption. If only one large or medium sized FI adopts PayThat and obtains 100% market share, the value of its PayThat Clearing Bank would be $28.64 billion to $32.8 billion and it could serve all End-Users globally that wish to adopt PayThat. If the maximum number of eight FIs purchase licenses and deploys a PayThat Clearing Bank and split the market share for PayThat services equally, for a modest investment to purchase a license, they would own a fee driven business that for each of the eight licensees would be worth $3.58 billion to $4.1 billion within three years if they achieve that average market share of 12.5%. These amounts move the needle for even the largest FIs.

Page 2: “Given the level of authentication required at enrollment and beyond, the customer registration experience with PayThat could prove to be overly complex and may impact end-user adoption.” As noted above, we will use best practice to achieve strong enrollment and strong authentication without discouraging adoption. The key to achieving this balance is to start at a commercially reasonable initial lower level of enrollment and authentication and then require customers to jump over additional hurdles when they wish to perform a transaction that poses more risk that the risk model allows without increasing the assurance of identity and authentication status. Academic research clearly indicates that customers have a high willingness to comply with additional requirements if they have a pending transaction that they wish to complete. See pages 25 & 32-33 of the proposal for more details.

Page 3: “But the limited number of Clearing Banks may hinder adoption, and the attractiveness of PayThat participation to potential FI partners is uncertain.” As noted in the next section, End-Users of non-participating FIs can adopt PayThat and the number of PayThat Clearing Banks does not hinder their ability to adopt. Non-adopting FIs will suffer loss of market share over time as PayThat grows. As noted above, the business model and value created by adoption is compelling.

Page 6: “Integration timeline estimates are not provided.” As noted above and on page 120 of the Proposal, in the PayThat use cases, the only points of integration are between the PayThat Clearing Banks, which serve as “edge servers” for traditional Depository Institutions and the payment systems of those traditional Depository Institutions. The integration required is equivalent to a banking corporate treasury workstation. The integration is modest and should only take weeks. By design and purposefully the amount of IT integration with the systems of legacy Depository Institutions is kept to a minimal level. Since most corporate treasury workstation solutions support data exporting and data importing, the challenge is mostly reduced to mapping and by using state of the art mapping automation tools, which have low six figure costs, the technical challenge is low and the technical risk is low.

Page 6: “The solution requires eight large banks to agree to act as PayThat Clearing Banks.” As noted above, one to eight domestic licenses will be sold. The system can be successful with just one PayThat Clearing Bank.

Page 7: “The lengthy, complex enrollment process ... may hinder adoption.” See the section above, “Achieving Strong Enrollment & Strong Authentication While Achieving Rapid Adoption”.

Page 7: “...the limited number of Clearing Banks may hinder adoption.” As noted below a single PayThat Clearing Bank can serve everyone in the entire U.S. since End-Users can access
accounts at any FI, whether those FIs participate or do not participate in PayThat. All FIs can join PayThat via correspondent service arrangements and market PayThat services to their entire customer base.

Page 11: “The proposal... does not indicate...the measures that will be taken [at these data centers] to meet FFIEC standards.” Page 49 and 50 of the proposal states, “The four databases and each PayThat Clearing Bank will be physically housed in enterprise network server data centers compliant with FFIEC standards for vendors for Depository Institutions. The data centers will incorporate (the following list is intended only to highlight at a high level some of the many FFIEC standards) policies, procedures and rules regarding:

- Physical security including physical access security
- Network monitoring and incident response
- Business disaster recovery and business resiliency & target availability plans and policies
- Enterprise level risk management frameworks and assessments including to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, payment system settlement and other risks across the end-to-end payments process
- Internal and external audits
- An annual Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, SSAE 16
- Periodic contingency testing and mock disaster scenario drills across the PayThat Payment System.
- Change management including those caused by technology and regulation changes
- Internal or external fraud or errors
- Periodic review and update
- Sigma 6 uptime, by ensuring all mission critical systems have geographically separated immediate fail-over redundancy, including POPs, servers and web services.

A full list of FFIEC standards can be reviewed by accessing the examiner guides of the FFIEC bank regulatory agencies. As a vendor to 373 other financial institutions, University Bank clearly has excellent FFIEC IT compliance.

Supplemental Information to Clarify Open Issues Noted by McKinsey’s Draft Evaluation:

Page 3: “It is not clear from the proposal whether the deposit account must be held at a Clearing Bank, or at a partner of a Clearing Bank.” If an End-User wants to establish a PayThat account at a PayThat Clearing Bank using a deposit account at a FI that participates in the PayThat Network, it is very easy using that End-Users existing electronic banking channels leveraging the SAML 2.0 standard single sign-in protocols.

However, a PayThat CashBox may be funded either with PayThat Tokens or with Good Funds transferred from any account at any FI accessible through a legacy payment system. If the account is at a FI that does not participate in the PayThat Network either as a Clearing Bank or as a correspondent of a Clearing Bank, enrollment is required prior to a PayThat Clearing Bank agreeing to debit this account. Enrollment of an account at a non-participating FI requires proof that the End-User actually controls this account. This is achieved using the “pushing pennies method” where a small deposit in a random amount between $0.01 and $0.99 is made via ACH
and the End-User accesses their deposit account using their existing method and enters the amount of the deposit transaction in the enrollment form. Now that the ACH system has moved to same day deposit, this method is much speedier than in the past and in the near future, will be even more rapid.

Page 3: “It is not clear from the proposal how recipients with deposit accounts at non-participating FIs will be able to access/withdraw their funds (U.1.1).” If an End-User wishes to withdraw funds from their CashBox and deposit it into a traditional deposit account at an FI, they must follow the same process described above to enroll the deposit account. Once enrolled, funds may be withdrawn from the CashBox and sent to their traditional deposit account at any FI, participating or non-participating. A fee for withdrawal is paid by the End-User and the funds are sent via ACH or Wire, depending upon how urgent the need of the End-User is, and how large a fee they wish to incur.

Page 3: “The proposal can be strengthened by clearly describing how smaller FIs will participate as indirect connectors to PayThat.” Small Financial Institutions can compete for new PayThat End-Users and contract for access to PayThat services for their existing customer base either through a large correspondent bank that owns a PayThat Clearing Bank or through the (at least) one PayThat Clearing Bank license reserved for a consortium of Small Financial Institutions and/or a Bankers Bank and/or a CUSO serving Small Financial Institutions. While a profit margin will be built into their business model, the typical bankers’ bank operates on a 5% Return on Equity business model, so the additional cost is modest. Competitive pressure from the eight licensees fighting for market share will encourage correspondent PayThat Clearing Banks to offer fair prices for access to PayThat services. There would be no service delays for small FIs working through a correspondent PayThat Clearing Bank. End-Users who adopt via a small FI should see no difference in quality of service as the End-Users of each PayThat Clearing Bank would be treated identically, except that the initial account enrollment is slower because while the PayThat Clearing Bank has immediate access to its own customer deposit data and the customer deposit data of participating FIs (via the edge server “network of networks” method), it does not have immediate access to customer deposit account data of End-Users who enroll traditional deposit accounts at non-PayThat participating FIs and has to use the “pushing pennies method” to enroll and authenticate the deposit account is controlled by the enrolled End-User.

Page 3: “The experience of end-users who hold an account in a non-Clearing Bank account should also be described.” End-Users who adopt PayThat and link PayThat to a traditional deposit account at an FI that is not a PayThat Clearing Bank should see no difference in quality of service as the End-Users of each PayThat Clearing Bank would be treated identically, except that the initial account enrollment is slower because while the PayThat Clearing Bank has immediate access to its own customer deposit data and the customer deposit data of participating FIs (via the edge server “network of networks” method), it does not have immediate access to customer deposit account data of End-Users who enroll traditional deposit accounts at non-PayThat participating FIs and has to use the “pushing pennies method” to enroll and authenticate the deposit account is controlled by the enrolled End-User.

Page 5: “The proposal can benefit from articulating how the solution leverages the Gateway functionality to drive the acceptance of cross-border payments, and how the solution will be interoperable with other real-time payments systems around the world (U.5.2).” As noted on
A GPG is constructed by having a bank be a member of the local ACH or Wire (RTGS) payment systems or possess a correspondent bank deposit account at a bank that is a member of each payment system in each country in which payments are to be sent or received from. This allows the bank to bypass SWIFT and using the real-time payment systems already built that connect to each bank in each country, to send or receive real-time payments globally.” As noted above, enrollment of linked traditional deposit accounts at FIs that participate in PayThat or accounts at FIs that do not participate in PayThat allows funds to move into and out of PayThat Clearing Banks from any bank account anywhere in the world where the GPG is connected into the local national ACH and Wire (RTGS) payment systems.

Because cross border payments routinely take one to two weeks to move funds across international borders, and there is no visibility for customers during the process until it is complete, by providing superior speed of cross-border transfers, transfers greater than the Western Union (and similar entities that have) transaction limit(s) of $10,000 will swiftly move from SWIFT to PayThat. Depending on transaction fees charged, the financial case for smaller transactions will also be compelling in certain circumstances. Small to medium size businesses and Small Office Home Office (SOHO) businesses will find these services most compelling, as larger firms that make large volumes of international payments are provided with higher quality service levels by their FIs. Please see the Replacement for SWIFT Use Case outlined above for more details on the adoption model and business model.

The design of the CashBox enables multiple accounts at multiple PayThat Clearing Banks. The PayThat Network rules will prohibit restrictions that prevent End-Users from switching PayThat Clearing Banks, restrict the use of multiple PayThat Clearing Banks or that place any competitive limitation on linked and enrolled traditional deposit accounts used to withdraw or fund a CashBox.

The proposal can be strengthened by clearly articulating how entities can easily switch between providers (E.1.3).” The design of the CashBox enables multiple accounts at multiple PayThat Clearing Banks. End-Users can establish accounts at any number of PayThat Clearing Banks. The PayThat Network rules will prohibit restrictions that prevent End-Users from switching PayThat Clearing Banks, restrict the use of multiple PayThat Clearing Banks or that place any competitive limitation on linked and enrolled traditional deposit accounts used to withdraw or fund a CashBox. An End-User may transfer from one PayThat Clearing Bank to another by enrolling and establishing an account with a new PayThat Clearing Bank, establishing an enrolled and linked traditional deposit account with that new PayThat Clearing Bank and then transferring any or all of the PayThat Tokens (good funds on deposit in the CashBox) to the new account via a PayThat payment, via email or SMS.

It can further be enhanced by clarifying the incentives for banks to become Clearing Banks; the proposer does state that each license would be worth $3.5-$4.1 billion in three years with a 12.5% market share, but it would be helpful to describe the assumptions for how a Clearing Bank would attain such market share.” One to eight PayThat Clearing Banks will be established in the U.S. market. If each had an equal market share and the maximum number of licenses was issued, each of the eight banks would have 12.5% market share. The four adoption use cases are designed to be able to achieve at least a 40% overall market penetration of that
market segment within 18 months. By pursuing the one to four of the adoption use cases, each PayThat Clearing Bank will take market share of payments from the legacy bank payment systems.

As noted above if only one large or medium sized FI adopts PayThat and obtains 100% market share of the four use cases detailed in the proposal, the FI, for a modest investment to purchase and build a PayThat Clearing Bank license, would own a fee driven business that would be worth $28.64 billion to $32.8 billion.

Page 6: “Further, it would be beneficial to explain how an end-user can fund a CashBox if they do not have an account at a Clearing Bank or at an FI that is associated with a Clearing Bank via a correspondent banking relationship.” This is described in detail above.

Page 7: “The proposal also states that “SWIFTNet runs an XML-compatible payment system with high transaction volumes without difficulty at comparable transaction levels to what VISANet handles [sic]” (page 132)” McKinsey has caught an error in our proposal. What we meant but did not write due to an editing error was SWIFTNet runs an XML-compatible payment system with high transaction volumes that could be scaled up further without difficulty to comparable transaction levels to what VISANet currently handles or to even higher levels in the future. SWIFTNet uses, among other techniques, XML compilers to speed XML calculations. XML to ASN1 to XML translators can also dramatically speed XML calculations. If it’s true we’ve only made one error in a 153 page proposal we’re pretty happy!

Page 8: “The proposal does not provide any tools to Clearing Banks for dispute resolution.” It is our understanding that FIs do not wish to have stand alone exceptions and investigations processes but wish to leverage existing systems and tools that they already use. For example, BSA Officers want data from all transaction systems to feed into a single searchable database that can monitor and detect fraud patterns in real-time or near real-time. The PayThat Clearing Banks will be able to share via edge servers and the “network of networks” design the data they require to be fed continuously into their existing exceptions and investigations processes instead of being forced to stand up a new and separate exceptions and investigations process just for PayThat.

Page 8: “The proposal could be enhanced by describing any available capability for Clearing Banks to search these databases for exception-related information.” All data in the PayThat databases will be fully searchable with results coming back variably based on role, authority and need to know parameters. Roles at PayThat Clearing Banks will be defined with different levels and types of access based on job requirements and authority and the data categorized and correlated with those levels and types of access so that access to the encrypted data contained in those databases is solely based on those role profiles and a need to know. Need to know is typically driven by an open investigative or customer service ticket caused by an open exceptions, dispute resolution or investigations process.

Page 8: “…the relationship between PayThat and the IAF is unclear. The IAF is not part of the network diagram on page 47 of the proposal.” As noted on page 137 of the proposal, “S.6.2: The Identity Assurance Federation manages the four PayThat Payment System databases.” The four databases are described in the network diagram on page 47 of the proposal. The IAF is the day-to-day operational arm of the PayThat Network. PayThat Corporation manages only the PayThat Network rules and collects license fees from the licensed Clearing Banks. Also as noted
on page 15 of the proposal, “PayThat Corporation will own all the required intellectual property or hold valid licenses covering all activities of the Payment System, End Users and Providers…” On page 21 of the proposal it is noted that PayThat Corporation will build the PayThat solution including the IAF’s functionality and the four databases. It will also assist the FIs that license a PayThat Clearing Bank with building those Clearing Banks and assuring initial interoperability. After the build out phase is completed, PayThat Corporation’s day to day operations other than licensing and management of the PayThat Network rules will be handed over to the IAF.

Page 8: “The proposal can be strengthened by articulating whether fraud monitoring occurs in real time or batch and explaining how information from PayThat servers is accessible to the IAF for monitoring. It would be helpful to explain in detail how PayThat and IAF work in conjunction to manage and monitor fraud - including detecting patterns at the individual or aggregate level (E.7.2).” Fraud monitoring will occur in real-time or near real-time both at the IAF level and at the individual PayThat Clearing Bank level. As noted above, the four PayThat databases will be fully searchable by the IAF and authorized personnel at the PayThat Clearing Banks with results coming back variably based on role, authority and need to know parameters. See above for more details. As noted above the IAF and the PayThat Clearing Banks and not the PayThat Corporation will manage and monitor fraud. Data will be fed from the four PayThat databases into existing industry standard fraud and pattern detection tools.

Page 8: “The proposal could be strengthened by addressing the incentives for operators and providers to manage the risk that they could pose to other participants (S.1.5), as well as by describing how the risk management framework will be periodically reviewed and updated while in production (S.1.6).” As noted on page 145 of the proposal, “Since the PayThat Payment System operates 24/7/365 and settlement via legacy ACH and Wire systems are not available on holidays and non-business days, the PayThat Payment System rules will require good funds to be held in central bank money escrow accounts in an amount designed by analysis and historical and projected flow of funds to ensure that sufficient funds are available to cover the net settlement risk among PayThat Clearing Banks and smaller Depository Institutions that are correspondents of PayThat Clearing Banks, to cover their obligations under Sigma 4, Sigma 5 or Sigma 6 probability, as determined by the PayThat Payment System rules (see page 44 of the proposal).” Because the size of the required deposit rises as the settlement risk rises and also as the volatility rises, PayThat Clearing Banks will be incentivized to take steps that will lower the required deposit, if those outweigh the financial benefit of making no changes to operational and/or marketing processes.

The risk management framework will undergo review annually or more frequently if needed based on the IAF’s assessment of risk, the effectiveness of risk controls and the net residual risk. If residual risk rises above acceptable levels (as defined in the risk management framework, review and revision will occur prior to the annual review date.

Page 10: “The proposal can be strengthened by outlining a minimum set of requirements for banks to follow in handling disputes of unauthorized transactions (S.5.1). There are concerns that a court proceeding may not be an effective way to handle disputed payments (e.g., handling them via operating rules may be preferable.” We agree 100% that End-Users should not have to resort to courts to settle issues related to disputes and exceptions related to electronic payments. The rules should mandate which entity has superior rights for all issues that could arise and a
dispute resolution mechanism that does not require court action. I once was told by a senior executive at VISA that VISA was a “dispute resolution mechanism that happened to move money”. However developing all these complex variations of the use cases into comprehensive rules requires community input and requires a great deal of detail that the various constituents need to weigh in on while finalizing the rules. (See L.2. Payment System Rules, page 50 of the proposal for the criteria that will be incorporated into the PayThat Network rules). We believe that the ECCHO rules are a good starting point and the Federal Reserve Faster Payments Task Force decision making framework a good starting point for the voting process governing the rule creation.

Page 50 of the proposal also states, “The PayThat Payment System rules that all Providers must agree and adhere to via a participation agreement, will ensure that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules, including those applicable to End-Users and that the PayThat Payment System can examine these institutions for compliance and has the ability and authority to sanction non-compliant entities up to an including termination of their ability to participate in PayThat, under network rules and procedures.” This will provide further assurance that each Depository Institution and each PayThat Clearing Bank adheres to all established applicable rules and does not disadvantage an End-User.

Page 10: “The Proposal can be enhanced by discussing the logic by which the IAF will monitor transactions and identify suspicious transaction patterns (S.6.3 and S.6.7).” As discussed above, data will be fed from the four PayThat Network databases into the existing industry standard fraud and pattern detection tools used by each FI that manages a PayThat Clearing Bank. It is our understanding that FIs do not wish to have stand alone exceptions and investigations processes but wish to leverage existing systems and tools that they already use. For example, BSA Officers want data from all transaction systems to feed into a single searchable database that can monitor and detect fraud patterns in real-time or near real-time. The PayThat Clearing Banks will be able to share via edge servers and the “network of networks” design the data they require to be fed continuously into their existing exceptions and investigations processes instead of being forced to stand up a new and separate exceptions and investigations process just for PayThat.

Page 10: “Additionally, the proposal would benefit from articulating the type of payment data that is available to be viewed (S.6.1).” As noted above, all data present in the four PayThat databases will be fully searchable with results coming back variably based on role, authority and need to know parameters. Roles at PayThat Clearing Banks will be defined with different levels and types of access based on job requirements and authority and the data categorized and correlated with those levels and types of access so that access to the encrypted data contained in those databases is solely based on those role profiles and a need to know. Need to know is typically driven by an open investigative or customer service ticket caused by an open exceptions, dispute resolution or investigations process.

Page 11: “The proposal... does not indicate where these data centers will be located (e.g., geographically dispersed locations)...” To be FFIEC compliant, for data centers of the systemic importance of PayThat, these data centers must be geographically disbursed at least 500 miles apart. It is assumed that the PayThat Clearing Bank data centers will be co-located at existing
FFIEC compliant data centers managed by the FIs that license PayThat Clearing Banks, with a primary and at least one (and probably two) fail-over location(s), each geographically disbursed.

Page 11: “The proposal can be further enhanced by providing details of a framework that will guide the composition of the solution’s managerial policies and oversight plans (S.7.3).” To establish its security control management framework, PayThat would incorporate NIST’s Risk Management Framework (RMF) Standard. This incorporates a risk-based approach that follows a six step process (as noted on the NIST website at http://csrc.nist.gov/groups/SMA/fisma/framework.html):

“Step 1: Categorize. **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis. [FIPS 199](http://csrc.nist.gov/groups/SMA/fisma/framework.html) provides security categorization guidance for [private sector] security systems.”

“Step 2: Select. **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions. [NIST Special Publication 800-53 Revision 4](http://csrc.nist.gov/groups/SMA/fisma/framework.html) provides security control selection guidance for [private sector] security systems.”

“Step 3: Implement. **Implement** the security controls and document how the controls are deployed within the information system and environment of operation.” Various other NIST standards would apply depending upon a variety of variables and requirements.

“Step 4: Assess. **Assess** the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST Special Publication 800-53A Revision 4](http://csrc.nist.gov/groups/SMA/fisma/framework.html) provides security control assessment procedures for security controls defined in NIST Special Publication 800-53.”

“Step 5: Authorize. **Authorize** information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. [NIST Special Publication 800-37 Revision 1](http://csrc.nist.gov/groups/SMA/fisma/framework.html) provides guidance on authorizing information system to operate.”

Step 6: Monitor. **Monitor** and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials. [NIST Special Publication 800-37 Revision 1](http://csrc.nist.gov/groups/SMA/fisma/framework.html) provides guidance on monitoring the security controls in the environment of operation, the ongoing risk determination and acceptance, and the approved information system authorization to operated status.”

Page 12: “The proposal could be improved by explaining how access to the solution’s databases will be supported, managed, or monitored (S.9.2-3).” As noted above, all data present in the four PayThat databases will be fully searchable with results coming back variably based on role, authority and need to know parameters. Roles at PayThat Clearing Banks will be defined with different levels and types of access based on job requirements and authority and the data
categorized and correlated with those levels and types of access so that access to the encrypted data contained in those databases is solely based on those role profiles and a need to know. Need to know is typically driven by an open investigative or customer service ticket caused by an open exceptions, dispute resolution or investigations process. Role definitions and standards and need to know definitions and standards will be reviewed and periodically updated, or more frequently as needed driven by user requirements.

As noted on page 137 of the proposal, “S.6.2: The Identity Assurance Federation manages the four PayThat Payment System databases.”

Database IT technical support, management, and monitoring is a standard financial services industry core competence and industry best practices and FFIEC applicable standards will all be utilized.

Page 12: “The PayThat solution will use the NIST 800-63-2 standard for enrollment and ongoing authentication of users and providers…. The standard has recently been replaced by 800-63-3.” While it is true that NIST has issued NIST 800-63-3 for public comment, it has not yet been finalized. When and if finalized, PayThat would use the NIST 800-63-3 standard for managing the enrollment and ongoing authentication process of users and providers. We would also incorporate any future updates to this NIST standard or any other referenced standards in the proposal, unless the updated standards are not commercially viable or practical to implement.

Page 13: “A detailed approach to managing credit and liquidity risk exposures is not described (F.4.1).” PayThat Clearing Banks only hold and transact good funds and operate on a 1:1 basis: for each PayThat Token in existence, there is 100% of the good funds represented by that PayThat Token on deposit at a traditional bank account controlled by the PayThat Clearing Bank. Settlement inside the PayThat Payment System is continuous and real-time both for on-us transactions inside a single PayThat Clearing Bank and for transactions involving two PayThat Clearing Banks. As a result because PayThat does not operate on a fractional banking deposit basis, but on a fully 1:1 good funds on deposit basis, there is zero net credit and liquidity risk in the PayThat Network. In the event that a Clearing Bank and its associated FI were to fail, the funds on deposit backing the PayThat Tokens that had not yet settled, would be held as fiduciary for the owner (the PayThat Clearing Bank that was due settlement of good funds) and payable to that owner if the FI and the PayThat Clearing Bank were liquidated. The escrow accounts in which the good funds are held would be entitled with some variation to cause a trust, escrow and fiduciary relationship for those funds held by the PayThat Network and not by the FI or its PayThat Clearing Bank alone. This may also facilitate the ability of the FIs that own PayThat Clearing Banks to earn the float interest income on the funds on deposit while keeping those deposits fully off-balance sheet, lowering capital requirements on the funds held on deposit in escrow.

Also, as noted on page 145 of the proposal, “Since the PayThat Payment System operates 24/7/365 and settlement via legacy ACH and Wire systems are not available on holidays and non-business days, the PayThat Payment System rules will require good funds to be held in central bank money escrow accounts in an amount designed by analysis and historical and projected flow of funds to ensure that sufficient funds are available to cover the net settlement risk among PayThat Clearing Banks and smaller Depository Institutions that are correspondents of PayThat Clearing Banks, to cover their obligations under Sigma 4, Sigma 5 or Sigma 6.
probability, as determined by the PayThat Payment System rules (see page 44 of the proposal).”
As noted above, because the size of the required deposit rises as the settlement risk rises and also
as the volatility rises, PayThat Clearing Banks will be incentivized to take steps that will lower
the required deposit, if those outweigh the financial benefit of making no changes to operational
and/or marketing processes.

The risk management framework will undergo review annually or more frequently if needed
based on the IAF’s assessment of risk, the effectiveness of risk controls and the net residual risk.
If residual risk rises above acceptable levels (as defined in the risk management framework,
review and revision will occur prior to the annual review date.

Page 14: “The proposal can be enhanced by clearly articulating whether the end user receives
the notifications via a push mechanism or the must be logged into CashBox to be aware of
them.” The CashBox would generate messages via push mechanisms when transactions are
received. For email based client interfaces, this would be an email notification. For mobile
device client interfaces, this would be a notification similar to what smart phone apps provide
when there is an event that the app provides updates regarding. Similar push mechanisms will be
established for other devices.

Page 14: “The proposal can be strengthened by describing a process for amending the rules
(L.2.2) and for resolving errors (L.2.5). The proposer should ensure that these processes are
addressed in the initial draft of the rules.” As noted on page 147 of the Proposal, “Within six
months of the commencement of initial work to build PayThat, a legal framework and
governance agreement (the “Governance Documents”) will be created that binds all the
Providers and End-Users of the PayThat Payment System. The following legal principles, rules
and policies will be incorporated into these Governance Documents: All laws, regulations,
regulatory interpretations or rulings, court decisions (collectively “Laws”) and/or PayThat
Payment System Rules that will apply to the Payment System, End Users, Providers, Payers and
Payees, and payments through the PayThat Payment System (page 50).” The Governance
Documents will contain a process for amending the rules and for resolving errors. This legal
framework and governance agreement is likely to be modeled on the ECCHO Rules Model and
we have received encouragement from ECCHO CEO David Walker in this regard. Decisions
required during the process of creating the Governance Documents will be made using the
Federal Reserve Faster Payments Task Force Decision Marking Framework, which is a highly
inclusive methodology. It is premature to build out or make additional decisions in this area
prior to engaging directly with the End Users and Providers including the PayThat Clearing
Banks who will initially adopt PayThat.

Comment on the QIAT’s Interpretation of Various Legal and Governance Criteria

In several instances, PayThat’s rating is noted as “Somewhat Effective” in the Legal and
Governance criteria because, for example, “The proposal acknowledges a need for a legal
framework and sets out a path to develop it (e.g., the legal framework is likely to be modeled on
the ECCHO Rules Model), but it is not yet complete. The QIAT has interpreted the Effectiveness
Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.””

Having served on the Legal and Governance sub work groups that built the Legal and
Governance criteria, I firmly disagree with the rating interpretation developed by the QIAT to
rank those proposals that have not developed completed rule sets but lay out a clear path to
developing compliant proposals as less than “Very Effective”. At no time during the discussion in these sub work groups was such an approach discussed and this is something that the QIAT has decided unilaterally without Faster Payments Task Force input. In fact, assurances to the contrary were made repeatedly during the criteria creation process in those sub work groups.

Summary
University Bank is pleased to present the Faster Payments Task Force community with a detailed, well thought out proposal that is highly rated by McKinsey. We do believe that our proposal fully meets all 36 criteria as “Very Effective” based on our understanding of, and participation in, each criteria sub work group and Task Force interaction during the process of creating the 36 criteria. Most importantly, our proposal not only lays out a superior technical solution, it lays out a business model and adoption model to achieve a creation of value many multiples of what was envisioned in the Federal Reserve’s whitepaper outlining the economics of adopting a new national more secure and faster electronic payment system. Over $30 billion of value can be created by PayThat, value that will accrue to the adopting entities.
UNIVERSITY BANK PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

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

At best, the University Bank proposal is aspirational in design and far from being tangible in fact. The mere fact that the proposer actively promotes a fund-raising effort within the proposal would suggest that the UB solution is slideware at best. Moreover, the ratings for rules, legal structure and modality, plus governance are overly generous since a guiding assumption is that the Fed will be the Central Network Authority, a huge leap of faith at this point.

Conceptual design. Avoids multiple effectiveness criteria, pushing multiple elements off onto the FED/Central Bank Authority for oversight on network, rules, governance, etc.

Interesting the funding request within the proposal—supports its aspirational design. Hopefully will take task force feedback to fill the gaps and improve.

Innovative cash purse system solution, but there are many limitations (e.g., dependent on Fed Wire, ACH, and contracted with at least 8-12 FIs for clearing) that could be a challenge in positioning University Bank as a Faster Payment solution.

It will be hard to motivate users to become members given the level of strict requirements. Also, requiring the unbanked segment to become banked could be a big hurdle, and, not necessarily the business models for the clearing bank/FIs. Would also require full support by ECCHO.

There is no substance to this proposal that I can understand. I am not sure how the QIAT did.

The assessment of this proposal is overly positive because the central function proposed has not been created, tested, completely designed, nor implemented. The proposal is a very good document for the means by which work could be undertaken to create what is envisioned. Without any experience in the space of creating or running such a system, confidence in the proposal along with timelines and the model itself seem questionable. I do not believe the QIAT could evaluate the solution, but only evaluate the proposed means of creating something without referent experience. In that, the proposal does well to present a means to design and create, but the effectiveness of the solution is, at best, in doubt.


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’s rules for risk management are not written. There is a 7x24 issue with clearing banks doing batch processing. The solution’s rules for legal and governance frameworks are not written.

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

I am agreeing based on the assumption that the solution will attract at least one clearing bank and become operational. (If that does not occur, the solution is not viable and would have no need to be assessed against the effectiveness criteria.) There are a few ratings which are too high - E3 - implementation timeline is not "somewhat effective" given the reliance on signing up clearing bank(s) and the need to identify a partner to underwrite development of the platform. Also - S5 - handling disputes - relies on FI processes, and that uncertainty does not merit an "effective" rating. The legal and governance frameworks are works-in-process. I do not agree with the QIAT’s arbitrary ratings for L1, L2, L3, G1 and G2.

While I generally agree with the QIAT assessment, I feel that the QIAT was too easy on the proposal. This proposal was another "thought experiment." The proposal document is full of maybes, plans, mights, wills. Even though the QIAT assessments were generally lower than the proposer's self-assessment, I still feel that the QIAT was too lenient. Given the difficulties in implementation, for example, the QIAT comments under Proposer's Ability to Implement were far too mild. And another concrete example: F4 - Fast Settlement. The QIAT rated the proposal as Very Effective, while admitting that there were significant areas missing and that there were still settlement and liquidity risk issues.

Agree as assessed. Solution is highly contingent upon securing 8 large financial institutions to act as the clearing entities, which may or may not be a good assumption and may or may not limit participation from other entities. Legal and Governance areas are still largely under development.

A very impressive proposal that would solve for the key criteria objectives IF a lot of pieces come together, including a licensing/funding proposition. The proposer’s self-assessment is clearly at odds with McKinsey's assessment, but given the complexity and the broad adaptability of the proposal, that seems like a footnote. Taken as a whole, I agree that McKinsey fairly assessed the proposal.

Legal and governance criteria need to be established, as assessed by QIAT.

Rules and governance are not fully described.
Very secure. Meets most of the ubiquity criteria. Uses text and email as ways to send and receive funds. Accounts pre-funded. Follows all FFIEC mandates. Addendum says they would work with ECCHO on governance framework. Interoperates with legacy system.

I would not rank settlement approach as very effective given it will be using existing systems which were not built with real-time payments in mind. Effective might be a better rating.

Contextual data capability is rated too highly – as multiple options are described, but does not describe how various parties decide upon and how they understand specifically what data to send and what data will be received by all parties. Rules and governance rated too highly, as details not provided. Comparatively, accessibility seems rated too low vs. other proposals, as it defines specific steps to reach all US bank accounts, given surety to payers that they can pay any other entity/individual.

Taken at face value and as a conceptual solution that has not been underwritten or built yet, I believe the assessment was correct. I like how it utilizes existing payment infrastructure for funding. Some areas were not fully addressed such as the rules, legal, and governance areas.

Overall OK but it’s not clear to me why a Somewhat Effective grading of 5.7? In the assessment, there was a request to explain measures to meet the required FFIEC standards. FFIEC standard describes the measures required to be compliant. Shouldn’t it be enough to just reference the FFIEC standard?

**TASK FORCE SOLUTION ENRICHING COMMENTS**

**Ubiquity**

I do have concerns around adoption of your proposed solution: The normal consumer will have difficulty understanding how this virtual "cash box" works and why it's necessary to have one to make payments he makes today. This could affect adoption...

I would have liked to see more details regarding the value proposition for financial institution participation, both as a clearing institution as well as a participating institution. I find it interesting the proposer, as a community financial institution, feels the need to rely on 8 large domestic clearing banks to carry out the mission. Additionally, currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. In order to be successful, University Bank will need to sell the solution to many of these providers. To date, these companies have been unwilling to do this without significant compensation, choosing instead to provide their own solutions. I would like to see a road map for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium-sized financial institutions.

The solution could be enriched by defining a strategic plan for acquiring the 12 clearing banks (8 domestic and 4 abroad) and the overall licensing process. Also, additional information on the business case for financial institutions to participate could be enriched as the proposed solution relies heavily on
financial institutions’ abilities to address consumer dissatisfactions, disputes, fraudulent transactions, and Regulation E issues.

Describe how all participants would understand the specific contextual data that flows with the payment so that all could consistently know what to expect in receipt of a payment – and/or how agreement on such is achieved by impacted parties.

The scheme proposes the concept of using email addresses and SMS text messaging for the transfer of funds which can help push ubiquity. However there are additional issues that need to be addressed. The proposal focuses on large clearing banks to interpret the transactions. 8 of these will be in the US and 4 international. What is the value proposition for these entities to take on this difficult task?

What was also somewhat unclear was how the registration process worked with FIs. Does an end-user have to have an account with an FI to register? Page 90 of the proposal mentions "Please select the bank you wish to register with." Does "bank" also refer to non-financial account holders? In essence, how is the registration process for unbanked or underbanked different?

Also somewhat unclear was how end-users with accounts at non-participating locations would withdraw funds they received via the proposal. Do they also have to sign up?

Lastly, the strong enrollment procedures seem as though they may be over burdensome and inhibit adoption. Forcing users to continually meet additional requirements as they become more "risky" could lead to some transactions being denied until additional measures are met. Will users follow through or just avoid this system? This might cause some users to become frustrated and resort to using other methods available. I just can't do x transaction there.

Unbanked segment would need to become banked, which may not be FIs' target segment or business model.

Conceptual.

Depends on ability to enlist 8-12 FIs to be clearing banks – could take some time and could involve a lot of resistance; longer than 18 months.

Doesn’t effectively address unbanked use case which covers significant portion of U.S. population.

Needs governance set up prior to implementation and ECCHO would need to formally support.

Because it is predicated on legacy bank systems, it would seem likely that ubiquity could be easily arranged, assuming participation from the banks.

Though there is a great amount of detail provided in the proposal, it would be beneficial to understand the user experience of customers of non-participating FIs and non-bank providers. Will there be a baseline customer experience for all customers? Will the baseline experience be available at the same cost for all customers? I can't help thinking there is a risk of financial inclusion by functionality yet exclusion driven by relative cost to the end-user.
In lieu of the authentication process outlined in the proposal, what does the consideration of a national directory or federation of directories do for end-user adoption?

**Efficiency**

The solution could be enriched if settlement and clearing could occur in a more real-time capability, outside of traditional ACH/wire.

Limiting the number of clearing banks will limit competition and drive up the cost to consumers. Consider having the Fed perform the clearing functions.

For value-added services, explain how they could be enabled in a way that would allow receivers of a payment to understand or anticipate what data-driven offerings would be coming to them.

Not sure how real-time clearing and settlement are done.

Relies on existing settlement parties.

Authentication at enrollment can be cumbersome for end-user experience, impacting adoption.

The limited licenses, and the accountabilities that come with them (customer inquiries, disputes, fraud, Reg.E) again call for a baseline customer experience along these lines and the structure to ensure that baseline is provided to ALL end-users at the same cost.

Settlement relies on participating FIs to work out how they want to handle vs. something well defined. Doesn't really address real-time settlement.

**Safety and Security**

Describe the timelines and communications to end-users when utilizing the outsourced fraud investigation services of the postal inspection service.

Unsurprisingly, Paythat checks all the boxes as it related to security and safety. It is clear that the designer of the PayThat solution is well-versed in the state of the art as it relates to payments security, and that concerns related to data security, authentication, enrollment, and privacy have been thoroughly considered and addressed.

**Speed**

(None)

**Legal**
I would have liked to see some suggested implementations for participation agreements and legal framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution could be enriched by including Payment System Rules and the legal framework needed for PayThat and CashBox (stored value account) to be successful. The overall solution could be enriched by describing the ways to retrieve funds from the CashBox.

Describe rules more specifically such that parties understand the impact on their roles and responsibilities.

Development of the legal framework will strengthen the proposal.

 Assumes US Post Office and others around the world will investigate fraud. Seems unlikely given taxpayer support and today's political environment.

**Governance**

I would have liked to see some suggested implementations for participation agreements, legal, and governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution could be enriched by detailing the solution’s governance related to the clearing banks and the user-controlled "cash purses."

Describe governance specifics.

As governance has not yet been written it is therefore lacking in detail. As an end-user I am strongly against using something such as ECCHO for governance which is not inclusive. Being an end-user we have a unique point of view and should be included in any governance including having a say on issues and voting. Without details it is difficult to say whether this is appropriate or not.

Development of the governance framework will strengthen the proposal.

The PayThat proposal addressed governance considerations very well, unlike many other proposals. The PayThat proposal explicitly stated that specific stakeholders or stakeholder groups should be able to "proportionately influence outcomes" and that the governance arrangements should provide for input and influence by all stakeholders. These references to influence are critical aspects, and a real strength of this proposal.

Ensure that the governance structure you propose aligns the interests of all participants to engage in your robust payments system.

Very light list of goals rather than actual governance plan.
G.1 Effective governance & G.2 Inclusive governance, NOT EFFECTIVE, challenging and “Within six months of the commencement of initial work to be build PayThat, a legal framework and governance agreement (the “Governance Documents: will be created that binds all the Providers and End-Users of the PayThat Payment System.

“PayThat System shall have the authority to examine and audit Entities and sanction and if necessary expel them from the PayThat Payment System for material uncorrected failures to adhere to the network rules. This independent examination and audit process will provide independent validation of compliance with the Solution’s rules, compliance with applicable law, and achievement of both the PayThat Payment System’s objective and public policy objectives.”
Proposer responses to the Task Force comments were optional and not all proposers chose to respond
Faster Payments QIAT

FINAL ASSESSMENT

Property of the Federal Reserve Bank of Kansas City and the Federal Reserve Bank of Chicago
(“Banks”)

Not for distribution or publication without the express written permission of the Banks
Faster Payments QIAT

FINAL ASSESSMENT

Proposer: University Bank

Summary Description of Solution:

University Bank describes PayThat, a closed-loop solution that provides good-funds transactions backed by funds held in a deposit account. PayThat is based on a system of end-user-controlled “cash purses” called PayThat CashBox, which is run by a network of networks (a set of licensed “Clearing Banks”) that interacts with but is separate from bank deposit, payment, and clearing systems. The PayThat system is built on top of, and interoperates with, existing legacy bank systems.

The solution is notable for its robust authentication of devices and individuals. It leverages email and SMS texting as ways to send and receive funds and their associated transaction data from a stored-value account (CashBox). Users’ accounts are prefunded to minimize risk through the transfer of funds from a traditional bank account. Funds are virtually present in the CashBox in the form of PayThat tokens, which are cryptographic artifacts that can be denominated in any currency (fiat or virtual). An identity management service called Identity Assurance Federation (IAF) maintains and encrypts users’ personally identifiable information (PII).

The solution depends on a limited number of Clearing Banks that will process and react to PayThat messages, interact with PayThat databases, send and receive payments from the domestic legacy payment system, and interact with other Clearing Banks. Once money is in the CashBox, it remains there, allowing transactions within the solution to be settled within the closed loop. The proposal indicates that twelve Clearing Bank licenses will be sold: eight to banks in the U.S. and four to overseas banks. The solution thus depends on eight large U.S. financial institutions’ agreeing to act as Clearing Banks. International transactions will be supported through a Global Payment Gateway that has not yet been created. The proposer maintains that the solution can launch within 18 months.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths

– PayThat is a highly secure solution with strong authentication of both the device and the end-user. The solution includes an Identity Assurance Federation (IAF) that contains all PII and potentially other information as well. This information is fully encrypted with clearly designed and controlled access levels. End-users have the ability to determine who can have access to their information.

– The proposal states that the PayThat solution is inexpensive for users to implement, operate, and maintain, and that it is less expensive to use than existing alternatives by at least 10x (p.11). The proposer claims that the solution can be built and rolled out to the market within 18 months, although it does need a partner to underwrite the initial platform development.

■ Areas for improvement and enhancement

– The solution requires net settlement in legacy funds when two PayThat Clearing Banks use a different depository to hold their escrowed funds. The solution relies on existing settlement capabilities (FedWire and ACH) and does not describe how a real-time clearing and settlement capability could be supported, if required. Settlement options vary within the solution. Individual transactions may be settled between Clearing Banks individually or in batch on a net settlement
basis, account to account, or by using an existing legacy payment system. (The proposal suggests that the preferred method would be ACH or FedWire.) If there is only a single Clearing Bank, funds will not need to be exchanged.

- Only one medium or large FI is required to successfully launch the system, and the solution has placed a limit on the number of Clearing Bank licenses to encourage early adoption of the solution. It is not clear, however, from the proposal how a single FI could adequately support the described potential market. The business case for FIs’ participation is unclear, yet the solution relies heavily on FIs’ abilities to address customer dissatisfaction, disputes, fraudulent transactions, Reg. E issues, etc.

- Given the level of authentication required at enrollment and beyond, the staged customer registration experience with PayThat could prove to be overly complex and may impact end-user adoption.

<table>
<thead>
<tr>
<th>Use cases addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>The solution addresses all four major use cases (P2P, P2B, B2P, and B2B) and includes cross-border capabilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposer’s overall ability to deliver proposed solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The proposer’s ability to deliver the proposed solution hinges on their ability to enlist FIs to serve as Clearing Banks and to participate and support the initial platform build. Also key to the solution’s success will be the effectiveness of viral marketing techniques to drive end-user adoption.</td>
</tr>
</tbody>
</table>
ASSESSMENT

Ubiquity

U.1 Accessibility

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

**Rationale:**

The solution consists of a pre-funded account called CashBox. Funds can be loaded through payments received from registered PayThat users, through cash or check deposits made at merchant partner locations, or through transfers from a traditional deposit account. The solution makes use of digital tokens that can be denominated in any currency.

PayThat allows users to load value from any type of account at any depository institution. A PayThat CashBox may be funded with good funds transferred from any account at any FI accessible through a legacy payment system. If the end-user’s FI is not associated with PayThat, the end-user must prove that s/he controls the account in question by enrolling in PayThat and then funding the account with a small deposit into the PayThat account. Regulated non-bank account providers are not permitted to be PayThat Clearing Banks (p. 45). Only licensed PayThat FIs can support clearing; they could therefore offer clearing services to non-licensed FIs.

Once the CashBox is funded, end-users can initiate payments to anyone using an email address, phone number or other supported alias. PayThat’s use of texting and email to send payments positions the solution to reach a significant portion of the “unbanked” population (U.1.4) as payees. If a payment is sent to a recipient who is not a PayThat user, the recipient will receive a marketing message inviting him/her to sign up for PayThat to access the funds. If an end-user with an account at a non-participating FI wants to withdraw funds from the CashBox account and deposit them into a traditional deposit account, s/he must enroll in PayThat, pay a fee, and move the funds via ACH or wire.

PayThat allows access to regulated non-bank account providers but requires those providers to hold funds in a master account at a depository institution (U.1.1, U.1.4). Moreover, funds cannot be deposited from CashBox into an account at a non-bank provider.

The solution supports cross-border payments and will also support multi-currency payments through its planned “Global Payment Gateway” (p. 54) (U.1.3).

PayThat can only attain widespread adoption if it succeeds in signing on several large depository institutions as PayThat Clearing Banks (U.1.5-6). It is unclear how easy this task will be. The proposal states that smaller FIs will participate as indirect connectors to PayThat via a PayThat Clearing Bank with a license to serve smaller institutions. The proposer indicates that competitive pressure from (eight) licensees fighting for market share will result in competitive pricing for smaller institutions.

The proposal claims that end-users experience the same quality of service whether they hold an account at a non-Clearing Bank or a Clearing Bank. The withdrawal of funds from the CashBox account will take longer for non-Clearing Bank account-holders. The non-Clearing bank end-user enrollment process requires substantial authentication steps, which may unintentionally hinder adoption.
PayThat has credible reach to end-users in that end-users can open accounts at PayThat Clearing Banks if their current FI is not a PayThat bank. But the limited number of Clearing Banks may hinder adoption, and the attractiveness of PayThat participation to potential FI partners is uncertain.

The solution is rated “Effective” here because partners must first sign on to bring the proposed use cases to life.

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:**

PayThat is device-, channel-, and platform-agnostic (U.2.1). A payee need only have an email address or SMS-enabled mobile phone to send and receive a payment (U.2.2). The solution is accessible to the end-user 24x7x365; the only requirement is internet connectivity that persists through the transaction cycle (U.2.3).

The solution allows end-users to use their existing devices and any assistive methods associated with those devices. The UI (user interface) is simple, with few options, but end-users can access higher levels of complexity as desired. 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, assuming users are comfortable with their existing devices (U.2.4).

The solution is flexible enough to be integrated into existing merchant acquiring solutions or to be deployed as a separate work-around.

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 core components of PayThat— the CashBox, PayThat Clearing Banks, eight messages, four databases, and the IAF’s enrollment and authentication services—deliver an end-user experience that is consistent across all channels (U.3.1, U.3.4). PayThat leverages email (SMTP) and text messaging (SMS) standards for communication at the end-user level (U.3.3). The error resolution process is predictable, as it is designed to address Regulation E and Regulation Z requirements (U.3.5). The solution is branded clearly as PayThat (U.3.6).

While the principles underpinning the operating rules are clear, it would be helpful to clarify whether the rules have been written and are in production (U.3.2) (p. 50).
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**

PayThat supports rich, XML-based, interoperable contextual data, as well as open APIs and help wizards to assist with interoperability and integration (U.4.1). The open API and help wizards automate the process of pulling data into standard industry business and personal finance systems (AP/AR, claims processing, payroll, treasury workstation, ERP systems, consumer accounting software, and tax reporting software) (U.4.2). The solution supports key industry standards for contextual data (e.g., STP820, ISO 20022, X12 data and UN CEFACT XML data), which is particularly important in helping to deliver the B2B use cases (U.4.3). XML data is captured and shared using the “network of networks” architecture and APIs to standard ERP systems (e.g., Oracle, SAP, Microsoft, etc.).

The proposal can be improved by more clearly detailing how the various data formats could drive advancements in the payment system with respect to contextual data and its potential uses.

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:**

A Global Payment Gateway—which has yet to be developed—is expected to facilitate a cross-border capability at implementation (U.5.1). The solution leverages ISO 20022 and UN CEFACT XML to support interoperability (U.5.2), and PayThat tokens can be denominated in any currency (U.5.4). PayThat Clearing Banks establish the solution’s exchange rates as an optional, value-added service. PayThat requires that all fees, rates, and terms be disclosed to the end-user prior to initiating a transaction, although it is left to the depository institution to provide the disclosure (U.5.3).

The proposal states that PayThat banks with correspondent relationships in other countries can use those countries’ existing real-time systems to send or receive real-time payments globally via their correspondent banks (U.5.2).

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:**

PayThat addresses the Faster Payments Task Force’s target use cases. Beyond that, the proposal outlines four additional use cases—with a detailed rationale for each—that go beyond traditional payments. The use cases are not considered to be within the scope of this evaluation, but they do demonstrate the extensibility of the PayThat solution.
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:
PayThat will grant eight Clearing Licenses in the U.S. based on an RFP process designed to accelerate and drive adoption. A single license may be held by a consortium of small FIs, a Bankers Bank, and/or a CUSO (credit union service organization) serving small FIs. Other non-licensed payment providers will be able to connect to PayThat through these Clearing Banks. It is not clear how limiting the number of Clearing Bank licenses may impact FI adoption. This design may restrict end-users’ choice among PayThat account providers (E.1.1).

The solution’s interface and messaging content are specifically defined and may leave little room for providers to differentiate. However, the end-user-facing PayThat interface makes it easier for entities to use multiple providers. The proposal does state that participating banks are required to disclose pricing when users enroll in PayThat (E.1.3).

End-users can establish accounts at any number of PayThat Clearing Banks, and system rules will allow end-users to switch Clearing Banks and hold multiple accounts. For end-users who do not hold a traditional deposit account with a PayThat Clearing Bank, switching providers or using multiple providers may be challenging (E.1.2-3). The proposal would be enhanced by clarifying the incentives for banks to become Clearing Banks. The proposer does state that each license would be worth $3.5-$4.1 billion in three years with a 12.5% market share, but it would be helpful to describe in detail how a Clearing Bank would attain such market share.

E.2 Capability to enable value-added services

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

Rationale:
PayThat supports the transmission and use of rich, XML-based, interoperable contextual data that can be leveraged to introduce additional services. PayThat also provides open, published APIs and help wizards that should allow payment service providers of all sizes to develop and provide value-added services, particularly data-driven offerings (E.2.1-2). PayThat’s operating rules require FIs to fully disclose any fees, etc. before fees are incurred, making the value proposition easily understandable to all end-users (E.1.3).

E.3 Implementation timeline

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

Rationale:
The proposal indicates that building the PayThat Clearing Bank software solution should take approximately six months. The proposer has intentionally designed the solution to minimize the amount of IT integration needed with FI legacy systems. Integration timeline estimates are not...
provided. The four databases contained in the solution can be built and tested in parallel and should also be completed in six months. To support cross-border payments, a Global Payments Gateway solution must be defined. The proposal suggests leveraging an existing global payment gateway operated by one of the major global banks (which would take one to three months) or building a GPG in partnership with a major global bank (six to twelve months). The total timeline seems to be about 12 months, with system operability and ubiquity increasing over the ensuing 18 months.

The solution can be successfully launched with a single PayThat Clearing Bank, but as many as eight large domestic banks may agree to act as PayThat Clearing Banks. The proposal would benefit by clearly articulating the initial incentives for a bank to join PayThat as a Clearing Bank.

The proposal assumes that existing bank operations/capabilities will be leveraged for customer complaints and fraud management. This assumption will need to be validated.

The proposal suggests an 18-month launch for PayThat but requires a partner to fund the building of the platform. The proposal indicates that funding should be readily available from the FinTech/venture capital community, or Depository Institutions could fund the cost of the solution themselves. (Total cost is anticipated to be less than $10MM.)

End-user growth relies heavily on a viral marketing approach based on enrollment by recipients of payments from PayThat users: to claim a payment, the recipient must enroll in PayThat. End-users will be required to jump through additional incremental enrollment barriers as they wish to do progressively larger and/or riskier transactions. The limited number of Clearing Banks may hinder adoption.

### E.4 Payment format standards

<table>
<thead>
<tr>
<th>Rationale:</th>
</tr>
</thead>
<tbody>
<tr>
<td>PayThat supports several key industry standards: STP820, ISO 20022, X12 and UN CEFACT XML (E.4.1). These formats enable cross-border interoperability (E.4.2), are cost-effective to adopt (E.4.3), are adaptable, and facilitate innovation (E.4.4).</td>
</tr>
</tbody>
</table>

### E.5 Comprehensive

<table>
<thead>
<tr>
<th>Rationale:</th>
</tr>
</thead>
<tbody>
<tr>
<td>In concert with FIs, which are responsible for various aspects of the end-to-end payment process, PayThat is able to deliver an end-to-end payment process from initiation to reconciliation (E.5.1). The Solution’s technical design supports all of its features (E.5.2). For transactions involving the conversion of PayThat tokens to fiat currency, the solution does not directly settle transactions but rather relies on Clearing Banks to use existing settlement mechanisms to determine settlement rules and windows between themselves (E.5.1-2).</td>
</tr>
</tbody>
</table>
E.6 Scalability and adaptability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
PayThat is expected to support the projected use cases (E.6.1), and the proposal asserts that the solution’s technical design is adaptable and flexible (E.6.2). It describes a “network-of-networks” architecture, but it would be helpful to provide more details about the hardware and software required to support the solution. The system’s messaging is based on SMTP and SMS standards, which have proven to be capable of handling millions of transactions per second and to scale well. The proposal also states that “SWIFTNets runs an XML-compatible payment system with high transaction volumes that could be scaled up further without difficulty to comparable transaction levels to what VISANet handles or to even higher levels in the future [sic]” (p. 132). The solution will be “stress-tested” quarterly at transaction rates 20x higher than historic peak volume.

The proposal can be strengthened by a technical explanation of how the system will scale (E.6.2). Additionally, providing insight into how the solution would adapt to future changes and needs in the payments system would be helpful to the proposal’s overall value proposition (E.6.3).

E.7 Exceptions and investigations process

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution relies on the PayThat Clearing Banks’ existing tools and protocols for exceptions and investigations to address customer complaints, fraud reports, and Regulation E issues (E.7.1-2). Because PayThat is available 24x7x365, Clearing Banks will have to expand their exceptions and investigations process to become 24x7x365 as well. This requirement may present an implementation challenge.

Transaction-related information is stored in PayThat servers and databases for seven years. This information is expected to be available to Clearing Banks to address and resolve disputes. While the proposal does not provide any tools to Clearing Banks for dispute resolution, the solution is designed to feed data required by the FIs into their existing exceptions and investigations process. This approach may require modifications to existing FI systems, processes, etc. The proposal could be enhanced by describing any available capability for Clearing Banks to search these databases for exception-related information.

The Identity Assurance Federation (IAF) is the day-to-day operational arm of the PayThat network and is responsible for managing the fraud detection system (p.137). Fraud monitoring will occur in real-time or near-real-time at the IAF level and at the individual PayThat Clearing Bank level. The databases will be fully searchable by the IAF and authorized personnel at Clearing Banks (based on role, authority). Data will be fed from PayThat databases into existing industry standard fraud and pattern detection tools. From the proposal, it appears that the IAF will itself own a complete set of these tools, feed data into these tools and leverage existing industry tools for fraud detection E.7.2).
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:

As designed, PayThat relies on robust end-user authentication, pre-funded accounts to support push payments, and blocked funds to support multiple settlement models. The risk management framework to be applied to the solution is thorough. The solution relies on pre-funded end-user accounts (S.1.2) to mitigate risk and on end-users to identify fraudulent transactions (S.1.4). However, the rules for risk management have yet to be written (although it is clearly stated that rules will be written within six months of the platform build). The risk management framework will undergo review annually, or more frequently if needed (S.1.6).

The proposal could be strengthened by addressing the requirements for operators and providers to manage the settlement risk that they could pose to other participants and the incentives/penalties for operators to allocate sufficient funds to support settlement when legacy infrastructure is not available (S.1.5).

S.2  Payer authorization

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

Rationale:

Payers can pre-authorize payments under certain parameters (S.2.2), revoke those payments in real time, or change payment parameters in real time (S.2.3). To promote safety and soundness, the solution requires authentication of both the device and the consumer (S.2.1). There are slight concerns that consumer authentication at Levels 3 and 4 (i.e., authentication of both device and consumer) may discourage usage and/or enrollment and thereby inhibit overall deployment.

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:

To ensure a “good-funds” model, the solution requires the Clearing Bank to validate the CashBox balance prior to initiating a transaction (S.3.1). Funds are available to the recipient as soon as the receiving FI accepts the payment. Given its use of pre-funded accounts, the solution meets the requirement that FIs or non-bank providers be compelled to approve payments after their initiation to assure the availability of good funds in the payer’s account (S.1.1). The payment becomes final and legally irrevocable once Regulation E’s time provisions have expired (S.3.2). Same-day ACH and the introduction of real-time payment networks are expected to expedite the payment’s finality.

The proposal could be improved by discussing the mechanisms and processes—beyond the Clearing Bank’s existing processes for dispute resolution—to protect or compensate the payer in the event of a dispute (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:**

PayThat holds stored value inside a PayThat account. This good-funds model essentially eliminates risk for all “in-system” transactions. The stored value is backed by good funds held within dedicated bank accounts that can only be credited or debited by the depository institution that holds the bank account. The dedicated bank accounts represent the activities of the CashBox accounts that are linked to them and support settlement in central bank money (S.4.3). The proposal assumes that the depository institutions would settle with the Clearing Banks periodically, based on accumulated balances owing or a time window. The proposal states that typical settlement would occur within 30 minutes or less (S.4.1). Settlement for transactions that move funds in and out of CashBox accounts may occur via ACH or FedWire, and amounts may or may not be net. Because PayThat is available 24x7x365, and current settlement capabilities are not, Clearing Banks will be required to hold sufficient good funds in central bank money escrow accounts to cover settlement obligations and to address settlement risk when clearing facilities are not operating (i.e., overnight, on weekends, and on holidays) (S.4.2). The solution requires Clearing Banks to settle using a pre-funded account or an approved credit line, which should eliminate the risk associated with imbalances in the payments system.

### 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 solution relies on existing FI processes to handle customer complaints, fraud reports, and Regulations E and Z issues. How these existing processes may need to be modified within participating FIs to accommodate PayThat accounts is unclear. The data stored in the solution’s four databases may be accessed via credentials differentiated by role, authority, authenticated status, and a “need to know.”

The proposal can be strengthened by outlining a minimum set of requirements for banks to follow in handling disputes of unauthorized transactions (S.5.1). There are concerns that a court proceeding may not be an effective way to handle disputed payments; handling them via operating rules may be preferable. The proposal suggests that the ECCHO rules will be used as a starting point.

### 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 proposal states that the IAF will facilitate timely, frequent information-sharing among all providers, operators, and regulators to assist in the management, monitoring, and mitigation of
fraud and evolving threats in accordance with applicable law (S.6.3). Moreover, PayThat payment rules will require the sharing of information to support the management and monitoring of fraud (S.6.1). PayThat captures transaction information, aggregates it in the IAF, and permissions access (S.6.6).

The proposal describes in detail how data owned by entities other than providers or operators would be aggregated, managed, and protected (S.6.2) (p. 137). The solution’s information-sharing mechanisms are easy to implement, update, and maintain, and they support differentiated access to content (S.6.4-5). The IAF is intended to manage fraud detection, which includes identifying patterns at the individual or aggregate level (S.6.7). The proposal does not define how patterns will be identified, however.

The solution will provide data to existing, industry-standard fraud and pattern detection tools and will monitor activity directly. (S.6.3, S.6.7).

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 proposal indicates that the PayThat solution will include strong technical access components and controls (S.7.1) (pp. 137-138), but the proposal can be strengthened by providing details as to how security requirements will be met. For example, the proposal states that the PayThat databases will be physically housed in enterprise-network-server data centers that are compliant with FFIEC standards, but it does not indicate where these data centers will be located (e.g., geographically dispersed locations). The proposal assumes that PayThat Clearing Bank data centers will be co-located at existing FFIEC-compliant data centers, and it further assumes that each data center will have a primary and at least one fail-over location(s).

The proposal provides a list of many FFIEC standards, policies, procedures and rules that will be incorporated into the data centers. It also provides detailed documentation of operational and procedural controls (S.7.2) (p. 138) and indicates that PayThat would incorporate NIST’s (National Institute of Standards and Technology) Risk Management Framework standard.

The solution can be further enhanced by providing more detail on the composition of the solution’s managerial policies and oversight plans to ensure that participants are meeting or exceeding requirements and incentives to do so (S.7.3).

S.8 Resiliency

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

**Rationale:**

The proposal describes a system that will deliver FFIEC-compliant policies and procedures for disaster recovery and business resiliency, but can be made more robust by detailing those policies and procedures (S.8.2-4). The solution will incorporate FFIEC requirements pertaining to Sigma 6 up-time (S.8.1) by ensuring that critical path systems will be geographically dispersed with
immediate fail-over capability. The solution will maintain different schedules—ranging from daily to annual—for specific tasks associated with resiliency testing (S.8.5).

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 requires that all data in motion and at rest be encrypted (S.9.1). PayThat is designed to ensure that end-users do not need to know each other’s account numbers to initiate or receive payments. Once an end-user has been “strongly enrolled,” no PII will be required to authenticate transactions (S.9.2-3). The proposal states that the PayThat Payment System’s four databases will store all data for seven years (or less if required by applicable laws and regulation). Monitoring and malicious-pattern-detection systems will protect all nodes in the system by monitoring for data breaches. (These systems will be selected following an RFP.) PayThat will require all data to be encrypted in motion or at rest, and access will be provided on a need-to-know basis based on role, authority, and authentication status (S.9.2-3). The proposal states that ASC-X9 Encryption Standards will be used to encrypt end-user data using methods known as Digital Rights Management (DRM). PayThat databases will be searchable, with access to data managed by role, authority and need-to-know parameters that will be defined based on job requirements and the data correlated with each role.

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 PayThat solution will use the NIST 800-63-2 standard for enrollment and ongoing authentication of users and providers. (The NIST standard provides technical guidelines for Federal agencies’ digital authentication of users who interact with government IT systems over open networks. These guidelines address only traditional, widely implemented methods for digital authentication based on secrets [per NIST website]. The standard has recently been replaced by 800-63-3.) The solution also aligns with FFIEC guidance and standards for authentication (S.10.1, S.10.3).

Per NIST, the level of identity-proofing assurance may rise from Level 1 through Level 4 based on the risk and dollar size of the proposed transaction. The solution supports robust authentication based on physical/biometric traits coupled with a personal possession that has been strongly enrolled and authenticated. The proposal indicates that the sender chooses the authentication method and can use any security method that is supported by the solution.
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:**
Providers must agree and adhere to rules via a participation agreement, but these rules have not yet been built. The proposal clearly states that the rules will be written within six months of commencing the initial build of the PayThat platform.

**Speed (Fast)**

**F.1 Fast approval**

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

**Rationale:**
The transmission and receipt of the solution’s eight payment messages should take less than two seconds, thereby meeting and exceeding the goals of the Faster Payments Effectiveness Criteria.

**F.2 Fast clearing**

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

**Rationale:**
The transmission and receipt of the solution’s eight payment messages should take less than two seconds, thereby meeting and exceeding the goals of the Faster Payments Effectiveness Criteria.

**F.3 Fast availability of good funds to payee**

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

**Rationale:**
The transmission and receipt of the solution’s eight payment messages should take less than two seconds. Authentication to the CashBox should take less than 30 seconds. The payee should then have immediate access to the PayThat tokens in the .pay file and to any contextual data the payee has rights to, based on the privacy template, authority, need to know, and authenticated status.
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**

PayThat Clearing Banks settle in real-time, but can agree amongst themselves to other methods, such as: (1) settling on a net basis periodically throughout the day when the accumulated amount owed exceeds $200,000; or (2) settling at intervals not to exceed 30 minutes as agreed between participating Clearing Banks (F.4.3). The Clearing Banks’ correspondent banks would provide cash balances or lines of credit to support these settlement options. No funds are ever required to be transmitted or settled via traditional bank payment systems (ACH, FedWire etc.).

The PayThat network is available 24x7x365. The PayThat system will require good funds to be held in a central bank money escrow account to support transactions that occur when legacy ACH and wire systems are not available (e.g., on holidays and non-business days). The size of the deposit required will increase as the settlement risk rises. The Clearing Banks will be responsible for managing their required deposit. These escrow accounts ensure that funds will be available to cover the net settlement risk among PayThat Clearing Banks and their correspondent banks (F.4.2).

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:**

As described, the solution sends notifications of payments to the payer’s CashBox (F.5.1). When a payment is made, the payee receives a push notification via email or text. The payment’s status is immediately visible to the payer as a pending, authorized transaction in the participant's CashBox (F.5.2). Once the payment has been accepted, the confirmation notifications are available within CashBox as well.

Legal

L.1  Legal framework

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

**Rationale:**

PayThat’s rules and legal framework have not yet been established, but the proposal describes a clear, thorough plan for building out the legal framework within six months of commencing to build PayThat. No existing rules or laws need to be changed to accommodate PayThat, as the solution will be designed to operate within the legal boundaries of the current payment system (L.1.2). The proposal cites no instances wherein end-users would perform the same functions in the payment system but would be subject to different banking and payment laws. All providers (Clearing Banks) must be FIs and therefore are all subject to the same applicable laws (L.1.5). The
PayThat System Governance Documents will define requirements where there is no definitive legal guidance currently in place.

The proposal acknowledges a need for a legal framework and sets out a path to develop it (the legal framework is likely to be modeled on the ECCHO Rules Model), but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.2 Payment system rules

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

**Rationale:**

As with the legal framework, the payment system rules for PayThat have not yet been written. According to the proposal, the rules will be drafted within six months after commencing work on building the solution. The proposal does discuss several key aspects of these rules, such as the fact that the PayThat system will have the authority to examine, audit, and—if necessary—sanction entities (L.2.3). The proposal states that the Governance documents will contain a process for amending the rules and for resolving errors (L.2.5).

The proposal acknowledges a need for payment system rules and sets out a path to complete them (the legal framework is likely to be modeled on the ECCHO Rules Model), but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.3 Consumer protections

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

**Rationale:**

Consumer protections are not defined in the proposal, as the legal framework has not yet been written. The legal framework and payment system rules to support error resolution will be drafted within six months of commencement of initial work to build PayThat. The proposal does discuss several key aspects of the system’s rules and specifically mentions Regulation E and Regulation Z. To the extent feasible, the legal framework will follow Regulation E and Regulation Z. It will be possible for Clearing Banks or the PayThat system to optionally establish additional consumer protections that exceed those required under applicable law.

The proposal acknowledges a need for consumer protections and sets out a path to complete them (the legal framework is likely to be modeled on the ECCHO Rules Model), but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
L.4 Data privacy

**Very Effective**        Effective             Somewhat Effective       Not Effective

**Rationale:**
PayThat and its developers have set forth a detailed, effective approach to data privacy, confidentiality, and security of payment and related data that includes user-controlled access and standard privacy templates (pp. 149-151). At enrollment, participants select a privacy template level that can be fine-tuned to the specific needs of an end-user or industry vertical (e.g., healthcare for HIPAA requirements). The .pay files use cryptographic standards so that each data element is separately encrypted and accessible solely based on role, authority, authentication status, and “need to know.”

L.5 Intellectual property

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**
Within six months of commencement of initial work to build PayThat, an intellectual property search will be performed. To date, a due diligence investigation has only been partially completed, with identified patents listed in the proposal (pp. 21-22).

**Governance**

G.1 Effective governance

Very Effective        Effective             Somewhat Effective       Not Effective

**Rationale:**
The proposer has not yet written governance documents for PayThat but will write them within six months of commencing to build PayThat. Based on the rules and policies outlined in sections G1-G4 and G2-G4 of the proposal, all required aspects of effective governance are expected to be incorporated into the governance documents.

The governance agreement is likely to be modeled on the ECCHO Rule Model. Decisions required during the development of the governance model will be made using the Federal Reserve Faster Payments Task Force’s decision-making framework.

The proposal acknowledges a need for effective governance and sets out a path to develop a governance model, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
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 proposer has not yet written governance documents for PayThat but will write them within six months of commencing to build PayThat. The governance framework is likely to be modeled on the ECCHO Rules Model.

The proposal describes key attributes of the proposed governance framework, acknowledges a need for inclusive governance, and sets out a path to develop such a framework, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”