Faster Payments QIAT

Proposer: SHAZAM, Inc.

February 21, 2017

TABLE OF CONTENTS

Original Proposal 2

Q&A Response 37

Draft QIAT Assessment 60
  (Includes proposer comment in Appendix A & B) 77

Task Force comments 80

Proposer response to Task Force comments 88

Final QIAT Assessment 94
Final Version
March 2, 2016

Faster Payments Task Force Proposal

Shared Success

April 29, 2016
Submitted by: Kevin Christensen, SHAZAM, Inc.
CONTENTS

Executive Summary ........................................................................................................................ 4
Use Case Coverage ......................................................................................................................... 5
   Supported Use Case Coverage Summary................................................................................ 5
   Cross-border Use Case Coverage ............................................................................................. 5
Proposal Assumptions .................................................................................................................... 6
Part A: Detailed End-to-End Payments Flow Description ............................................................. 8
   Part A, Section 1: Solution Description .................................................................................. 8
      1. Initiation ........................................................................................................................ 9
      2. Authorization and authentication ................................................................................. 10
      3. Clearing and receipt ....................................................................................................... 10
      4. Settlement and reconciliation ....................................................................................... 11
   Part A, Section 2: Use Case Description ................................................................................. 13
      1. Business to Business (B2B) ....................................................................................... 14
      2. Business to Person (B2P) ............................................................................................ 15
      3. Person to Business (P2B) ............................................................................................ 16
      4. Person to Person (P2P) ................................................................................................. 17
   Part A, Section 3: Use Case by Effectiveness Criteria ............................................................... 18
Part B: Business Considerations ................................................................................................... 20
   1. Implementation Timeline ............................................................................................. 20
   2. Value Proposition and Competition ............................................................................. 23
   3. Integration Effort ............................................................................................................. 24
Part C: Self-Assessment Against Effectiveness Criteria ............................................................... 26
   1. Ubiquity .......................................................................................................................... 26
   2. Efficiency ....................................................................................................................... 28
   3. Safety and Security ......................................................................................................... 30
   4. Speed .............................................................................................................................. 33
   5. Legal Framework .......................................................................................................... 34
6. Governance ................................................................................................................. 35
EXECUTIVE SUMMARY

As one of the original pioneers of real-time debit transactions, SHAZAM is pleased to have the opportunity to provide a proposal to enhance the payments system.

SHAZAM’s proposal leverages many tried and proven components of the existing payment to allow for a more rapid realization of the task force’s goals in speed, security, and efficiency. It allows for continued innovation in access devices, form factors, and delivery channels for future proofing ubiquitous access. It introduces some small, practical tweaks in governance that can help ensure collaboration and deliver an extremely high degree of inclusivity and interoperability.
## USE CASE COVERAGE

### 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 Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>Remittance for accounts payable, purchases</td>
<td></td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>Insurance claims, government benefits, payroll</td>
<td></td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>Bill payments, purchases</td>
<td></td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>Funds transfer to friends, family, or small businesses; A2A interbank funds transfer</td>
<td></td>
</tr>
</tbody>
</table>

### Cross-border Use Case Coverage

<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>Any country not sanctioned by the Office of Foreign Assets Control (OFAC). The solution has several networks from which participants may choose to conduct a cross-border transaction.</td>
<td></td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Same as above.</td>
<td></td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Same as above.</td>
<td></td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Same as above.</td>
<td></td>
</tr>
</tbody>
</table>
Proposal Assumptions

1) Traditional ATM and debit card networks have transitioned to become more comprehensive, general purpose payment networks.
2) Functional interoperability is attainable today if the networks are required to share transactions similar to ACH operators.
3) Two or more financial institutions that exchange transactions directly are a de facto network and should fall under the same requirement to share with other networks.

Innovations in access devices and their form factors have blurred the lines of distinction in labels for types of networks. Just last decade, a company like SHAZAM would be called an ATM network. Certainly, SHAZAM is a payment brand that supports ATM transactions. However, an increasing number of those transactions are no longer conducted with a card or even at a terminal. We assert that a card number is simply a payment account token that may exist with or without a physical card. This has in fact been done in the past. For example, SHAZAM has allowed bill payment and internet banking providers to originate real-time balance inquiries, funds transfers, and bill payments using payment account tokens. The depository financial institutions participating in the program associated payment account tokens to the depositors’ accounts but did not necessarily provide cards. Some implementations use one-time tokens for e-commerce purchases. New devices such as smartphones and wearables can have tokens provisioned without the need for a physical card. Debit card networks now operate on much broader array of transaction sets, channels, and form factors than arguably any comparable class of network. They are more appropriately described as payment brands that can debit and credit accounts in real-time using either real or tokenized account identifiers.

While the breadth of participation in these debit networks is great today, there remains a problem of interoperability. Virtually every depository financial institution participates in a debit network, and with Regulation II, it is required to participate in at least two networks. Yet unless a participating financial institution joins every payment brand, he cannot be assured a successful transaction. An accountholder may attempt a transaction with a service provider whose sponsoring financial institution does not participate in a brand that is in common with the accountholder’s depository financial institution. This first type of interoperability problem is caused by a payment brand participation gap. It is not feasible that every financial institution join every possible payment brand to ensure full ubiquity. Most payment brands already have existing interconnections. Functional interoperability is achievable now, using these interconnections, without requiring every participating financial institution to join every payment brand. When one payment brand facilitates a transaction into another payment brand, it is called sharing. We suggest adoption by the industry of a rule that requires sharing. A similar provision in NACHA — The Electronic Payments Association®’s rules, Subsection 4.1.7, ensures
interoperability of ACH. By requiring networks to share transactions, the payment brand participation gap would be closed.

A second type of interoperability gap stems from a lack of adherence to payment brand rules. Some financial institutions choose not to accept certain transaction sets that are otherwise mandated by payment brands. They may have their own proprietary solution, or they may want to require originators to join their scheme in order to have access to their accountholders. Unfortunately, these financial institutions can have considerably large deposit bases and may share with each other and exclude the rest of the ecosystem. This creates fragmentation and discriminatory access to the payment system. When two or more financial institutions interchange a type of transaction, they have implicitly established a de facto network. If they are classified as such, and required to share with their peer networks, the financial institution participation gap is closed.

Neither of these gaps are a consequence of economic or technical challenges. They are the outcomes of dominant market participants acting in their proprietary interests. Our assumption is that the faster payments system will benefit most from the principled requirement that there be universal sharing and equity in participation.
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

Part A, Section 1: Solution Description

Financial institutions participate in one or more networks and agree to adopt their network rules. An end user may participate in the payment system by opening an account at a depository financial institution or a regulated non-bank account provider that is sponsored by a participating financial institution.

Payment service providers may participate in the payment system by being sponsored into a network by a participating financial institution. The sponsor financial institution is responsible for the service provider’s adherence to network rules and is liable for its settlement activity. The network exchanges cryptographic keys with the service providers and any intermediary processors to ensure they are authenticated. They may enter into agreements with end users that grant them authorization to initiate transactions using a payment account token that is recognized by a participating financial institution. Service providers may charge end users fees to participate in the service as long as they are disclosed properly.

The networks regularly distribute directories of payment account token prefixes to service providers and processors. They use the directories to determine if they may route a payment through a particular network. End users’ account numbers and other sensitive information are not distributed. The end user maintains control of his or her identity and with whom the information is shared. The proposal does not depend upon any new directory capabilities; however, new concepts that extend the existing directories could be applied. For example, networks could also act as central node operators and payment account tokens could be the destination account information that payees register in a directory such as that envisioned by the Remittance Coalition’s B2B Directory Project.
The following diagram is a generalization of the payment process, which may be applied to several use cases. The baseline features provide real-time delivery of guaranteed, good funds from payer to recipient with full availability of funds to the recipient.

1. **Initiation**

A payer may initiate the transaction through any number of channels or access devices. The user must have a payment account token that is enrolled in the service. The service provider will ask the payer to provide the identity of the recipient, which could be a social networking ID, cell phone number, or email address. The payer can create ad hoc, scheduled, or recurring payments. The service provider must provide a means to cancel scheduled or recurring payments.

If the recipient is enrolled, the payment may proceed. If the recipient is not enrolled, the service provider will contact the recipient so he or she may enroll in the service. During enrollment, the recipient provides a destination payment account token. At no point do the payer or recipient discover each other’s account numbers or sensitive information.
Payer or recipient accountholders may have accounts domiciled at depository financial institutions outside of the United States or denominated in a different currency. The system has several networks that have established messaging that conveys to each party its transaction amounts in its respective currency. Correspondent banks assist the networks in their cross-border settlement using a prevailing, wholesale currency conversion rate.

2. Authorization and authentication

The service provider may prompt the user to provide credentials to access the service. It is incumbent upon the service provider to comply with the applicable state and federal laws and regulations of applicable administrative authorities. The service provider must implement appropriate anti-money laundering compliance and OFAC screening. It must also comply with network operating rules, including the institution of velocity controls and risk mitigation measures.

The service provider may proceed with the payment request when the recipient’s destination payment account token is on file. The service provider first debits the payer who wants to send money. The debit authorization may include information used to authenticate the payment account token or the sender. The network will route the debit authorization to the depository financial institution or to another network if necessary. During authorization processing, the depository financial institution will verify funds availability, verify any authentication values passed by the service provider, post the debit to the account, and respond to the network. The network responds to the service provider, which is then able to begin the process to credit the recipient.

3. Clearing and receipt

The debit to the payer’s account may be disputed by the accountholder as specified by both Regulation E and applicable network operating rules. The liability rests on the financial institution that sponsored the service provider into the network. The payer accountholder’s depository financial institution may adjust or return the debit if it was unauthorized. The network provides a facility for the adjustment, which may be submitted using automated messages or manually entered in a portal. In some cases, the network rules may allow for the liability to be shifted to the payer accountholder’s depository financial institution if certain authentication values are passed for authentication during the authorization. In these cases, the payer’s depository financial would not have the right to return an unauthorized debit.

Credit transactions are warranted and cannot be reversed by the originator. When the recipient depository financial institution receives a credit, it may perform risk management (including anti-money laundering) to decide whether to approve or decline the transaction. The transaction
should be posted immediately after its approval. The recipient depository financial institution is required to provide immediate, full funds availability to the recipient. The recipient depository financial institution confirms to the network that the credit was successful. This step allows the network and service provider to finalize the transaction and provide confirmation to end users. If the transaction was not approved, which may also be due to a timeout or system error, the service provider will reverse the debit to the payer’s account.

The proposed solution today uses the ISO 8583 message specification. New functionality and message types can be added to new standards, such as ISO 20022. Support of prior functionality can be carried forward on legacy standards until participants have migrated to the new ones. While the industry as a whole generally uses ISO 8583 today, virtually every network has its own implementation, often called a dialect. Processors and financial institutions use integrators and in-house developers to map messages so they may move seamlessly from one endpoint to another through differing dialects. This is a core competency of networks, integrators, and processors. ISO 20022 simply represents a different standard that requires its own message mapping. This proposal is distinguished more by its governance principles than technical implementation. If the business needs dictate, then the networks comprising the solution will adopt the appropriate supporting standards.

4. Settlement and reconciliation

The network performs settlement on a daily basis using ACH or wire transfers for some participants. The settlement amount is a net of all of a participant’s debit and credit activity during the period. Based on historical activity, the network uses a formula to calculate daily prefunding amounts to ensure sufficient liquidity to compensate for any differences in inter-network settlement windows. Settlement activity reports and reconciliation files are distributed to participants to assist in daily reconciliation. Participants in a transaction know to which settlement period it belongs by the value in the message that identifies the settlement date. Some scenarios merit more rapid settlement to minimize settlement risk or manage liquidity. A payer may request a transaction be eligible for immediate, gross settlement or an intra-day net settlement batch conforming to intervals specified by the network (such as hourly). The service provider may indicate the settlement frequency in the transaction request message. The payer depository financial institution may factor a transaction’s settlement frequency in its decision to approve or decline the request. If the transaction is approved for real-time or intra-day settlement, the network will use a real-time gross settlement (RTGS) facility such as Fedwire® provided by the Federal Reserve Bank. Settlement reporting will need to be iterated on the same frequency as the intra-day intervals. The reports will need to identify items and totals that were real-time or in a particular intra-day batch.
In addition to the reporting and reconciliation data, the network provides transaction history. A portal provides financial institutions a means to research transaction details and process exception items. The network monitors for irregular patterns, and can notify the financial institution (or on its behalf, individual accountholders) of suspicious activity.

Consider the SHAZAM® BOLTS™ application as an example service. The application is licensed to several hundred financial institutions. The financial institutions allow users to add payment account tokens so they may send or receive money through the service. SHAZAM BOLT$ may be accessed through a web browser, Apple® iOS device, or Android® device. The application authenticates users with login ID and password; however, participating financial institutions have the option to increase authentication on higher value payments using secure, out-of-band method to capture an authentication code. The application provides a means for the financial institution to provide its end user terms and conditions, and it collects and reports on their acceptance. Each financial institution may establish its own fee structure, and the application provides for disclosure of the fee at the time of the transaction.

**SHAZAM BOLT$ Send Money feature**
Part A, Section 2: Use Case Description

In all of the following use cases, the service provider role may be a financial institution or a non-bank entity sponsored by a financial institution. If the service provider is a not a financial institution, it must be sponsored into the network by a participating financial institution.

Financial institutions and their service providers should perform a risk assessment for their policies and procedures, including fraud prevention, anti-money laundering, and risk management. They must obtain the licenses, registrations, and approvals from the appropriate regulatory authorities. Cross border activity should be monitored for suspicious activity. End users should be screened to ensure they are not on watch lists and any applicable transfer limits should be enforced.

As stated earlier, it is a fundamental governance assumption that the networks will interchange transactions. We do not depict the sharing in the use cases, because the activity is transparent to all of the actors except for the networks. To facilitate sharing, the networks exchange directories and provide the union of their payment account token prefixes in their distributions to service providers and processors. By participating in one network, the end users have the ability to transact across all networks.

As discussed in section 1, none of the use cases require that a payer know his recipient’s sensitive information, including account number. Both parties will enroll with service provider, who will associate identities with payment account token information. The service provider is expected to provide sufficient data security to protect payment information from compromise and ensure user privacy is not violated. If a payer attempts to initiate a payment to a Recipient not yet enrolled, the service provider or payer may contact the recipient and request he enroll.

In some of the use cases, the process map has steps that are highlighted in green. These are optional steps depending upon a service provider’s particular implementation. In some cases, the payer may have a banking relationship where sufficient credit is in place to allow the service provider to send credits without having obtained prior authorization for offsetting debits to the payer’s account. The service provider may also have a prefunding agreement in place with the payer to minimize settlement risk.
1. Business to Business (B2B)

The payer in a B2B transaction may have remittance data that is required by the recipient to recognize the payment. The payer or its service provider may include the information with the transaction. If the information is sufficiently complex, it may be appropriate for the transaction to simply convey the location of the remittance data. The Recipient could then retrieve the remittance detail from a URL provided in the transaction rather than from the transaction itself.

The diagram below depicts both options, where the network would use ISO 20022 remittance advice information or remittance advice location.
2. Business to Person (B2P)

The B2P process is materially similar to B2B, but it lacks the requirement to convey remittance details.

<table>
<thead>
<tr>
<th>Business to Business payment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payer</strong></td>
</tr>
<tr>
<td>Initiates transaction</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Authenticates end user</td>
</tr>
<tr>
<td>Requests debit to end user’s account</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Provides confirmation to recipient</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Authorizes, posts debit, and responds</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Authorizes, posts credit, and responds</td>
</tr>
</tbody>
</table>

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
3. Person to Business (P2B)

Similar to the B2B use case, the service provider may need to collect and provide remittance detail for the payment to be posted by the recipient. The detail may be provided by directly by payer. The payer may include his remittance information, such as an account number with the recipient, when he initiates the transaction. The service provider may also provide a means to provide the details on behalf of the payer. For example, the service provider may provide an invoice presentment to the payer. The payer may access and respond to the invoice presentment through an application, such as internet banking. The proposal allows the flexibility for other implementations, such as a mobile bill payment application that scans QR codes for remittance detail from an invoice.
4. **Person to Person (P2P)**

At the completion of a successful transaction, the service provider should provide both Payer and Recipient notification. The recipient needs the notification to alert him of the increase to his available funds. The use case does not require remittance details be provided to the recipient. However, some implementations may allow the payer to provide a memo with the payment. The service provider passes the memo to the recipient in the notification.
## Part A, Section 3: Use Case by Effectiveness Criteria

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.10</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Payer Authorization</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Approval by the Payer’s Provider</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>F.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>F.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Clearing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</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

The timeline consists of the following distinct phases and durations.

- Phase 1: Governance – 2 years
- Phase 2: Basic interoperability – 1 year
- Phase 3: Commercial enablement – 2 years

Phase 1 – Governance

The proposal calls for the use of a system that is readily available today, for the most part, with several incumbent network operators to provide for competition and innovation. The key assumption is that the industry would universally adopt a measure similar to the rule requiring ACH operators to exchange batches and entries.

Networks have varying competitive attributes, such as brand value, membership structure, operating rules, and fee structures. For there to be competition, it is appropriate to allow continued variability. However, to achieve interoperability, there does need to be common governance for the shared network arrangements. If there is not common governance, then not only may functional interoperability fail, but some participants and networks may also discriminate in pricing or network access to the detriment of others. The universal sharing arrangement must provide a backbone that level sets messaging, backstops against predatory pricing, and insulates against discriminatory access. Networks will still be free to differentiate on the value they provide within their networks, but the value of their inter-network capability would be universal.

It is possible the effort to erect and maintain the universal sharing rules could be absorbed by an existing industry association, such as the National Automated Clearinghouse Association (NACHA). If there is not a suitable incumbent willing to fill the governance requirements, then it may be necessary to create a new not-for-profit rules-making organization. This process could be steered by the Federal Reserve Bank and include representatives from industry stakeholder organizations, such as the American Bankers Association, Independent Community Bankers Association, Credit Union National Association, Debit Network Alliance, Merchant Advisory Group, and Remittance Coalition. A membership organization
could be created, and its dues could be used to fund operations required to administer its operation. The organization should also reserve some seats for public sector representation. The organization would have a limited stock ownership structure or otherwise define its voting rights in a manner that ensures equal representation and control by all classes of stakeholders. Work groups and standing committees would be organized from among the membership. Ad hoc work groups may be created for special initiatives. Standing committees with rotating memberships would be required for rules, pricing, risk, and specifications. Members may be asked to agree that their contributions become property of the association to ensure that association work may be available for public use without intellectual property rights risks. Members may also be competitors, so the association will need policies that prohibit members from engaging in activities or discussions that may be anti-trust violations.

Networks require financial institutions to execute participation agreements binding them to adhere to the operating rules as well as any applicable laws and regulations. The agreements also hold them responsible for the compliance of any service provider or processor they sponsor. The operating rules of incumbent networks can provide a starting point for the rules committee to structure the rules of the universal sharing arrangement. Operating rules articulate responsibilities for network participants, including the requirement for service providers to honor payers’ requests and obtain and document their authorization. The rules have provisions that specify liability on a transaction, the requirements for error resolution, adjustments, and the dispute process. The rules committee could draw on much of these existing network rules to create a consensus, normalized set of rules for the participants of the universal sharing arrangement. Network agreements would need to be amended to include pass-through provisions required in support of the universal sharing arrangement.

The risk management committee would monitor systemic risks in the universal sharing arrangement. It would be responsible for the policies and procedures used to evaluate member network credit, liquidity, and operations to mitigate counter-party risk. The risk management committee may recommend risk related rules, pricing, penalty fees, or other sanctions to enforce its policies. It would document business continuity standards for member networks. It would also document data security, end-user privacy and data protection standards for all participants. The risk management committee would administer the inter-network fraud reporting system. It may be a centralized, consortium model that is staffed by the association or outsourced to a third party. It may also be possible to define a federated model, where a common specification allows for the networks participating in the universal sharing arrangement to exchange the data amongst one another without the need for a centralized repository.

At this time, there does not appear to be a mandate (either statutory or regulatory) that would compel networks to share transactions. It is our hope that this proposal will be a catalyst for
the industry to coalesce in good faith around the principles of network sharing to advance the cause of the faster payment initiative. We applaud the Federal Reserve Bank and the Faster Payments Task Force on their leadership in organizing this proposal process. If they deem this proposal of value, perhaps their influence may help gain the cooperation of a critical mass of networks to share. If we were to obtain a critical mass, it is likely that all financial institutions and networks would determine it is in their best interest to participate.

If there is a good-faith effort by industry participants, it should not take more than two years to establish the governance framework for universal network sharing.

**Phase 2 – Basic interoperability**

The proposal leverages the existing debit networks to attain basic functionality rapidly after the completion of Phase 1.

Basic functionality includes the following capabilities.

- Use cases
  - B2P
  - P2P
- Commercially available options for form factors, access devices, and delivery channels
- Flexible authentication options
- Real-time payer authorization with acknowledgement
- Real-time clearing with acknowledgement
- Ability to immediately notify payer and payee of receipt
- Efficient daily net settlement using ACH and Fedwire
- Mature back office processes
  - Settlement activity reporting
  - Reconciliation files
  - Exception item processing procedures
  - Arbitration processes
Phase 3 – Commercial enablement

Following Phase 2, the networks build the capabilities required to accommodate commercial transactions.

- **Use cases**
  - B2B
  - P2B
- Add the ability for originators to request real-time settlement on a transaction
- Add the ability for networks to override a transaction’s default settlement period to real-time or an intra-day batch
- Enhance interfaces to transport ISO 20022 remittance advice or remittance advice location information
- Enhance payment account token directories with commercial feature attributes
- Produce settlement reports and reconciliation files intra-day
- Provide revised interface specifications to service providers, processors, and financial institutions

The message extensions may be adopted optionally by service providers and processors that wish to support the commercial use cases. The intra-day and real-time settlement will also impact financial institutions that are accustomed to daily back office cycles. This phase may be two years in duration for the networks to complete their changes. It may take several more years for all financial institutions and their core software providers to certify and fully support the extensions. Any solution will benefit from an ability to support incremental participation. To facilitate it, the network directories of payment account token prefixes should indicate to service providers and processors which payee routing options support the commercial enablement features.

2. Value Proposition and Competition

At the heart of this proposal is the realization that the industry needs healthy competition. For that reason, this proposal puts its focus on a governance model delivering universal sharing. It provides a means for all financial institutions to have parity in their access to the payment system. There will be a continued need for the sponsorship of service providers, which is a source of revenue for financial institutions. However, financial institutions may not be required to join several networks in order to ensure their service providers can originate a transaction to any recipient. Financial institutions may focus on one or two sets of network operating rules instead of several unless the business case merits it. Networks also administer interchange fees as a means to encourage financial institution participation. This will be necessary to fund the type of investment that financial institutions will make in their systems.
to realize the full capabilities envisioned by the faster payments initiative. However, due to the presence of a shared network, there will be a natural backstop to unreasonable interchange rates. The prevailing rate of the shared network becomes the ceiling for the remainder. This benefits the service providers, end users, and society as a whole.

Certainly, a major source of revenue for networks is in transaction processing. Networks stand to benefit from the potential growth in transaction volume associated with the addition of new use cases in the proposal. Perhaps more importantly though, we believe most networks will also benefit from a more level playing field. Networks compete for financial institution business on a number of factors — principal among them are their breadth of acceptance, transaction switch fees, and interchange fees. These factors generally accrue benefit to whomever has the largest scale of operation. The bigger a network becomes, the more opportunity it has to use its size to its benefit. The proposal benefits networks by allowing them to compete on aspects other than size. They may compete on branding, service, innovation, operational excellence, or efficiency. Networks would not have to be amongst the largest to be viable. It opens the door for new market entrants by lowering the barrier of entry.

Service providers may benefit from the structure as well, because they may no longer require multi-network sponsorship arrangements. They may experience decreased sponsorship expenses and more predictable, standardized network operating rules. Service providers may continue to enter into agreements and charge various service fees to payers.

End users, payers and payees, will benefit from a more seamless, fully ubiquitous real-time transaction with real-time funds availability. They may also see reduced payment expenses if the efficiencies described are realized by service providers.

### 3. Integration Effort

The scope of Phase 2 is attainable without impact to most stakeholders except the networks. A financial institution must participate in one or more networks. The integration may require a financial institution or its technology provider to develop an interface with the network. The process generally takes about four months to complete. Most financial institutions have already integrated with one or more networks in a capacity that supports Phase 2 of the proposal. End users, service providers, and processors may also use existing interfaces and business arrangements. Networks may choose to implement the integration required for Phase 2 through either direct interfaces or commercially available gateways that consolidate interfaces to multiple networks. It is a business case decision that a network may make based on the amount of inter-network activity expected in a particular relationship. This type of implementation is a relatively straightforward effort with successful examples both past and present.
The scope of Phase 3 may require a significant duration of effort and investment by all stakeholders. B2B end users and their technology providers will have to make changes to their systems to create the payment instructions, include remittance details, and potentially automate initiation of the transactions into a service provider’s solution. We would expect P2P service providers to insulate consumers from any changes with the adoption of the new, faster payment solution. Consumers may just need to be presented with an option to expedite a payment, perhaps at a premium, by providing a payment account token from a participating financial institution. Financial institutions that receive payments including remittance data will have to make modifications to their commercial banking and cash management solutions. They will need to include the remittance advice or remittance advice location information for the business receiving payments. The businesses receiving payments may also require changes to their interfaces to receive the remittance data. Financial institutions or service providers may help mitigate these changes by mapping the information into pre-existing, legacy interfaces.

The availability of optional, varying settlement frequencies introduces new considerations for all stakeholders in the transaction. If it was not explicitly requested by the payer, a service provider would need to ensure the payer knows and agrees to his or her offsetting debit being effective for a more expedited settlement option. Payer financial institutions will require that notification rules be in place at the networks to manage their prefunding and liquidity in their settlement accounts. The service providers, processors, networks, and financial institutions will all need to recognize new settlement indicators (real-time, daily, or intra-day batch) within the transaction message. This will require development and certification.

We expect some service providers and end users to rapidly adopt these changes due to the increased utility and efficiency they offer. This will provide an incentive for financial institution adoption in order to be positioned to maintain commercial accounts.
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

1. Ubiquity

Self-assessed rating:

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

Justification for U.1:
The solution allows financial institutions to associate payment account tokens with varying account types. The accounts may be sponsored into the payment system by a financial institution on behalf of regulated non-bank account providers. The solution has widespread adoption with several networks, thousands of financial institutions and service providers, and millions of end users. The proposal increases its utility with new commercial use cases and enhances its interoperability with an improved governance model.

Justification for U.2:
The solution is device agnostic. It already has integrated several channels with varying device types and form factors, both physical and virtual. The solution allows for innovation in identity management and its linkage to payment account tokens. The recipient registers his own payment account token and associates it with his identity, which may include such items as email address, name, telephone number, or whatever attributes a service provider and its end users deem appropriate. Service providers have built a variety of applications to accommodate varying user types, including accommodations for individuals lacking technical proficiency, having disabilities, or conversing in foreign languages. The networks
all operate on a high availability, 24x7x365 basis. The network funds transfer credit rules operate on a good funds model. The recipient is to receive immediate funds availability. The recipient’s depository financial institution is guaranteed settlement.

**Justification for U.3:**
The network rules provide documentation of standardized expectations relative to baseline features and requirements. Network rules stipulate that financial institutions and their service providers are responsible for end user terms and disclosures.

**Justification for U.4:**
Phase 3 provides network support to convey contextual data from the payer or payer service provider to the recipient depository financial institution. The use of the ISO 20022 remittance advice and advice location specifications will provide a standard that stakeholders may depend on for integration efforts. Service providers, technology integrators, businesses, and financial institutions may innovate in their applications but still have an anchor in the standard that passes the payment and the data.

**Justification for U.5:**
Existing networks that operate on the scheme have multicurrency, international access. If they are included in the inter-network sharing arrangement, their end users may participate in cross-border transactions with the participants of all other networks.

**Justification for U.6:**
Phase 2 of the implementation supports P2P and B2P. Phase 3 adds support for B2B and P2B.
2. Efficiency

**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>Efficiency</td>
<td>E.1</td>
<td>Enables competition</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.2</td>
<td>Capability to enable value-added services</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.3</td>
<td>Implementation timeline</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.4</td>
<td>Payment format standards</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.5</td>
<td>Comprehensiveness</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.6</td>
<td>Scalability and adaptability</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.7</td>
<td>Exceptions and investigations process</td>
</tr>
</tbody>
</table>

**Justification for E.1:**
The proposal lowers the barrier of entry for new networks to enter the market and levels the playing field for competition among the networks, without regard to their size or duration of incumbency. The uniformity and interoperability afforded by the shared network governance model provides the ability for financial institutions, processors, and service providers to convert from one network to another without significant impact. The more frictionless portability will provide for increased competition among networks.

**Justification for E.2:**
Service providers may be sponsored into networks by financial institutions. The proposal not only allows but rather depends on service providers to extend the baseline functionality through their applications to realize its full potential. There are examples of service providers that have already used the proposed system to provide convenient and innovative solutions.
**Justification for E.3:**
The baseline features are to some extent already in the market if the users accept some compromises in interoperability. Service providers and financial institutions have attempted to cover these gaps by joining multiple networks. The plan and timeline to reach Phase 2 and Phase 3 are realistic given the head start in infrastructure and participation enjoyed by the incumbent networks.

**Justification for E.4:**
The proposal calls for a governance model supporting universal sharing between the networks. The networks currently use ISO 8583 which is sufficient for use through Phase 2 of the implementation. Phase 3 of the implementation makes use of the ISO 20022 remittance advice and remittance advice location standard.

**Justification for E.5:**
The proposal addressed all stages of the payment process. This has been demonstrated in the market for the baseline features.

**Justification for E.6:**
The existing technical design supports functionality through Phase 2 of the implementation, and the Phase 3 description discussed changes required to support the commercial use cases. The networks are built for high availability and have demonstrated their capabilities to absorb peak demand. All of the networks operate in a dynamic market, where rapid change has been required to implement disruptive innovations and regulatory mandates. They have demonstrated their ability to meet these challenges.

**Justification for E.7:**
The network provides access to transaction history for research, and to procedures and facilities for exception item processing.
3. Safety and Security

**Self-assessed rating:**

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

**Justification for S.1:**

*Member networks and financial institutions already have robust compliance and risk management functions that address these issues. The proposal calls for the formation of a*
not-for-profit association that would have a risk management committee with the power to enforce its recommendations on members through operating rules, fines, and sanctions.

**Justification for S.2:**
The network allows service providers to obtain real-time authorization from payer depository financial institutions. The debit is posted in real-time to the payer’s account, and it is visible immediately through teller, internet banking, or mobile banking applications.

**Justification for S.3:**
The credit sent by a payer are warranted by the financial institution that sponsors the service provider. The recipient depository financial institution is guaranteed good funds. A payer maintains the right to dispute unauthorized debits with his depository financial institution. Depending upon the type of authentication used by the service provider, the payer depository financial institution may be able to adjust the transaction with the service provider’s sponsor financial institution. Network rules determine which party has liability depending upon the authentication factors that may have been present at the time of authorization by the payer depository financial institution.

**Justification for S.4:**
Financial institutions are responsible for settlement of activity associated with their sponsored non-bank or service provider participants. Financial institutions that participate in a network will have provided the network permission to originate settlement transactions on their behalf. Networks manage liquidity with prefunding formulas that adjust based on participants’ historical activities. The association will have a risk management committee that will define safety and soundness policies ensuring networks participating in the inter-network sharing are protected from counter-party risks.

**Justification for S.5:**
Existing network rules define dispute policies and procedures. The association for inter-network sharing will harmonize these rules.

**Justification for S.6:**
Proposal is flexible to a consortium model that is centralize or federated with the scope defined by the association for inter-network sharing.

**Justification for S.7:**
Networks have policies in place for security controls, which may be leveraged and harmonized for enforcement amongst participants in the inter-network sharing arrangement.

**Justification for S.8:**
The networks have business continuity plans that are regularly updated and tested.
Justification for S.9:
The networks use payment account tokens and do not require account number or personally identifiable information be passed with the transactions. To the extent a service provider, processor, or network handles sensitive information it must comply with Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry (PCI) requirements.

Justification for S.10:
The network can accommodate varying authentication methods. The network rules often define liability based on the method of authentication that was used on a transaction. Service providers and financial institutions may adopt methods that suit their use cases and risk tolerance.

Justification for S.11:
Member networks already undergo audit and examinations. As members of the association for inter-network sharing will agree to pass-through provisions that drive association rules down to their member financial institutions, processors and service providers. The association’s risk and rules committees may institute processes to field grievances, monitor compliance, and sanction members who do not comply.
4. Speed

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

**Justification for F.1:**

Network rules require financial institutions to provide the network a response in less than 10 seconds. If they do not, the network is authorized to stand-in on their behalf to ensure quality of service to the end user. The vast majority of transactions are processed in far less time than the network mandated maximum duration. For example, the SHAZAM network average response time for the full transaction cycle is only 400 milliseconds. This time includes SHAZAM receiving the service provider request, routing the request to the financial institution for authorization, and returning the authorization response to the originator.

**Justification for F.2:**

The network uses a single message transaction which is posted by the financial institution at the same time it is authorized.

**Justification for F.3:**

Network rules require the recipient’s depository financial institution to provide full funds availability immediately upon receipt.
Justification for F.4:
The proposal provides for the network prefunding to help manage liquidity risk. The proposal provides optional, expedited settlement. The payer may specify more rapid settlement subject to authorization approval by the payer depository financial institution.

Justification for F.5:
The network provides service providers and their processors real-time responses from payer and payee depository financial institutions. Service providers may provide immediate notification to the end users. The SHAZAM BOLT$ example provides an immediate response to the user on screen, and both the payer and payee receive an email notification.

5. Legal Framework

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>Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.1 Legal framework</td>
<td>x</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.2 Payment system rules</td>
<td>x</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.3 Consumer protections</td>
<td>x</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.4 Data privacy</td>
<td>x</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.5 Intellectual property</td>
<td></td>
</tr>
</tbody>
</table>

Justification for L.1:
The proposal calls for the use of existing networks, which have established rules and compliance functions that ensure they comply with relevant laws and regulations.
**Justification for L.2:**
Existing network rules from incumbent networks address these issues; however, the not-for-profit organization that establishes the rules for the universal sharing arrangement may ensure all of these provisions are pass-through requirements.

**Justification for L.3:**
Network rules specify liability and dispute procedures. The rules for the universal sharing arrangement may provide additional pass-through provisions.

**Justification for L.4:**
Existing network policies may remain as a baseline. The rules for the universal sharing arrangement may provide additional pass-through provisions.

**Justification for L.5:**
Members will agree that any contributions to the association become association property.

### 6. 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># Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Governance</td>
<td>G.1 Effective governance</td>
<td>x</td>
</tr>
<tr>
<td>Governance</td>
<td>G.2 Inclusive governance</td>
<td>x</td>
</tr>
</tbody>
</table>

**Justification for G.1:**
The proposal suggests industry formation of a not-for-profit membership organization with rules-making authority for its participants.

**Justification for G.2:**
The rules-making organization will be structured in a manner that provides equal representation and voting rights on important issues such as rules, pricing, and specifications.
Faster Payments QIAT

PRELIMINARY ASSESSMENT

Proposer: SHAZAM, Inc.

APPENDIX A: QUESTIONS TO PROPOSERS
Questions posed by the QIAT with proposer responses inline.

Ubiquity

U.1 Accessibility

■ What will the end-user experience look like once all debit networks are sharing transactions?

– Today, service providers, processors, and their sponsoring financial institutions must join and connect to virtually every network to ensure that their merchants can accept payment from anyone or their payers can send payment to anyone.

□ This adds overhead through additional participation fees and the maintenance of physical network connections. Service providers and processors may be forced to ration network access, creating fragmentation – cases where the merchant may not be able to accept a payment or a payer may not be able to send a payment – because the network is not supported.

□ Under the proposal, service providers and their processors may use a single network to provide access to any accountholder through universal sharing. They may still make business case decisions to build direct connections to specific networks if it is more advantageous than the sharing option. For example, a network may charge the processor or its sponsoring financial institution an additional gateway fee to gain access to other shared networks. They may find a direct connection more cost-effective. This model helps ensure cost-effective access to the payment system for transaction originators. (U.1.6)

– Today, end users experience cases where they are unable to complete a transaction.

□ The end user may be attempting to make a purchase at a retailer whose processor is not a member the same network as the end user’s depository financial institution.

□ The end user may be attempting to send money to a payee but the service provider is not a member of the same network as the payee’s depository financial institution.

□ The end user may be attempting to send money to a payee, and its processor is a member of the same network as the payee’s depository financial institution; however, the payee’s depository financial institution does not support the network’s P2P transaction.

□ Under the proposal, an end user may conduct transactions without concern about it failing due to fragmentation in the payment system. (U.1.2)
What is the minimum number of networks that would need to participate in this Solution to deliver the scale necessary for success?

- The objective is to eliminate fragmentation and discriminatory access to the payment system, which requires all networks to participate.

Will this Solution require that an FI participate in multiple networks, or would access to all participating networks be available through each participating network?

- Financial institutions may be able to join one network to originate transactions and have access to any accountholder through universal sharing. As noted in the previous section, there may still be business cases for some direct connections.

- Although this proposal is not applicable to debit cards alone, it is our opinion that applicable Regulation II alternate brand requirements would still require a card issuer to be a member of two or more payment brands.

What is the approximate investment required by each network participant and each Provider to support the implementation of this Solution?

- Network operators would implement sharing. Service providers, sponsoring financial institutions, and processors may take a status quo approach and make no changes. If they want to realize opportunities to decrease expenses, they may decommission interfaces and consolidate connectivity through a single network that provides universal access. We see no cost and only benefit to service providers, processors, and financial institutions.

- A number of sharing relationships already exist amongst the existing networks. ACH operators are already required to share transactions.

- Networks would bear the cost to create any new shared network connections that may be required. Most already have technical connectivity to peer networks to send and receive transactions through a processor business context. Those same interfaces may be used to support a shared network context.

- Networks that do not want to undertake the development effort may use a gateway. They may make a business case decision based on their effort and the amount of volume they have with another operator.

- Networks that do choose to develop new interfaces to another network will have messaging, settlement, billing, reporting, and exception item processing logic to build. From our experience, these types of projects may be anywhere between 1,000-1,500 hours of cross-functional effort (business, project management and development time resource time).

U.2. Usability

Will the Solution require the same coverage of channels, devices, and transaction types across all networks and FIs?

- The solution does not require specific channels and devices. They are determined by service providers with some constraints by network rules or applicable regulations.

- The transaction set for universal sharing should support all transaction types. The governance body will need to define which are mandatory.
How will the Solution ensure that there is consistency in the aliases offered across all of the networks so that end-users can be certain how to route the payment?

- Similar to maintenance of routing numbers or IIN/BIN ranges, networks and processors will be able to determine route available using a payment account token. This will ensure consistency across networks for the purpose of facilitating transactions.

- An accountholder’s depository financial institution may provide multiple tokens that are associated with the same account. Specific tokens may be created for specific service provider relationships.

- The payment account token may suffice as an alias that is consistent across networks.

- The payment account token may be used in online wallets, cards, mobile phones, wearables, and other devices that may be support contactless payments.

- End users may enter into agreements with service providers where they knowingly share personally identifiable information such as a mobile phone number or email address as an alias. The solution helps protect personally identifiable information by not requiring it to be shared outside of the service provider.

U.3. Predictability

Will all participating networks be obligated to provide the same functionality for end-users (channels, devices, transactions)?

- The solution does not require specific channels and devices. They are determined by service providers with some constraints by network rules or applicable regulations. Within acceptable bounds, end user experience may vary, so service providers may have a means to compete on feature differentiation.

- The transaction set for universal sharing should support all transaction types. The governance body will need to define which are mandatory.

How will the Solution support clear, compliant documentation and communication of baseline features to end-users, and/or how would the proposer have to modify the Solution’s rules to achieve this goal?

- Networks would align operating rules with those of the universal sharing arrangement.

- Service providers will be required by network rules to provide consistent disclosures to their end users.

Will end-users be able to route payments across all participating networks using the same set of aliases?

- Payment account tokens may be used as alias and they would work across all networks.

- Other aliases that use personally identifiable information would be truncated at service providers. An end user may choose to use the same alias across service providers. In either case, the service provider would enter the transactions into the networks using the token which would support routing across networks.
Will there be a single dispute process that will apply to all participating networks?

- An accountholder would dispute a transaction through its depository financial institution.
- If deemed appropriate, the depository financial institution may perform exception item processing with the network.
- If the transaction was “out-of-network,” meaning it was a shared network transaction, then the depository financial institution’s network processes the exception item with the other network.
- The process is consistent to end users whether or not the transaction was shared.

How do the proposer’s existing rules support consistency in error resolution, and how would the proposer have to modify them to achieve this objective?

- Network rules stipulate conditions that permit a participant to submit a transaction for exception item processing. Service providers provide consistent experience to end users by adhering to the rules.
- Each network will need to harmonize its error resolution rules with the sharing agreement to provide for consistency.

Will the network be visible to end-users? If so, how will this network be branded to support end-user awareness?

- No, the intent is not to create a new brand. The solution would enhance existing network brands through sharing.
- It is our experience that end users do not associate branding with their ability to conduct transactions. For example, in today’s environment, branding at the point-of-sale is inconsistent. The retailer may not display all brands that are accepted. It may display brands that are not accepted. End users simply expect their cards to work.
- The proposal would improve the current state, because the end user would be assured that he could facilitate the transaction with the brand provided by his depository financial institution.

U.4 Contextual data capability

- Will minimum standards be established for contextual data at the network level?
  - Yes, this is envisioned for phase 3.

- Will debit network participants, participating FIs, and service providers be required to support new message types enabled by ISO 20022?
  - Yes, this is envisioned for phase 3.
U.5 Cross-border functionality

- Which non-US domestic debit networks have been solicited and found interested to investigate joining the effort
  - We have not collaborated with any networks in our preparation of this proposal.

- What are some of the key steps that must be taken to leverage the capabilities of some networks’ cross-border capabilities?
  - The easiest solution is to allow the network that has the cross-border capability provide for currency conversion. The transactions are performed to each party in their own native currencies. It is transparent to the domestic network, service providers, and end users.

- What is the proposed timing for cross-border transaction support?
  - Phase 2

- Would participating networks with cross-border capabilities be required to provide cross-border access to other debit networks as a participant in the Solution?
  - If a network operates in the US, it would be our position that it should be in the sharing arrangement and interoperable with other networks.

- How will you ensure that end-users of all networks understand clearly the timing of funds availability and all costs associated with a cross border payment?
  - Depository financial institutions provide accountholders disclosure of any fees associated with currency conversion on cross border payments.
  - Service providers and networks may offer currency conversion value-added services to allow end users to lock in specific conversion rates for a transaction.
  - No different than with domestic transactions, timing on funds availability is determined by the cross border network operating rules and is communicated to end users by service providers.

U.6 Applicability to multiple use cases

[No questions]
Efficiency

E.1 Enables competition

[No questions]

E.2 Capability to enable value-added services

■ Does the proposer intend to require that certain value-added services be developed centrally and made available to all participating networks, or will each network develop new products and services for its end-users only?
  – It is not envisioned that there will be centrally developed services.
  – Networks may create their own value-added services as a means of differentiation to win direct connection from service providers and financial institutions.
  – Service providers will have many more networks that can provide universal access from which they may choose.

E.3 Implementation timeline

■ How will the Solution change in terms of scope, timeline, and impact if networks are not mandated to share transactions?
  – The timeline is not dependent upon the number of networks in the sharing arrangement.
  – The scope and impact are decreased proportionally by the percentage of networks that would not join.

■ How will the Solution change in terms of scope, timeline and impact if the definition of network is not modified to consist of 2+ financial institutions that exchange transactions directly?
  – There would be no impact to the proposed timeline.
  – The scope and impact may be decreased to these particular financial institutions, because fewer sharing interfaces would be required.

E.4 Payment format standards

■ Please prepare a more definitive plan to support ISO 20022 in order to support the transmission of contextual data and cross-border transactions.
  – It is our intent that ISO 20022 be adopted in phase 3 between networks.
  – Service providers, processors, and financial institutions may adopt it over time as dictated by the use cases they are supporting.
E.6 Scalability and adaptability

- Is the proposer expecting a significant volume increase across the networks? How will the Solution handle large volumes on the interconnection between networks? Please discuss TPS rates, adding throughput capacity, etc.

  – Networks already enjoy significant year-over-year increase in transaction growth. It is not clear that the universal sharing of transactions will more rapidly increase the growth of transactions in the payments ecosystem.

  – They use fault tolerant, highly scalable systems that operate well under capacity. It is common for networks to have the capacity to process anywhere from hundreds to thousands of transactions per second.

  – Networks, processors, and financial institutions often have redundant connections.

  – Network engineers monitor activity to ensure that processor and network interfaces have sufficient capacity.

E.7 Exceptions and investigations process

- How will the existing networks’ rules and solutions to handle exceptions be aligned to deliver a consistent end-user experience across networks and their participating FIs?

  – Networks will continue to maintain their own exception item processing rules and systems.

  – Exception items for shared transactions will be processed by networks – it is transparent to the users.

  – The universal sharing agreement will have rules that networks must adhere to and promulgate amongst membership. This will normalize end-user experience across networks.

- If possible, please provide some high-level requirements or guidelines for a centralized/federated solution. Describe which parties would have access to the data, and how end-users could monitor or control access to their transaction information.

  – A number of networks participate in similar systems today, where a third party receives transaction information, including the disposition of the transactions (good or fraudulent). The information is used to identify trends that may be shared with participants. The information may also be used to improve predictive models.

  – The organization governing the universal sharing arrangement can dictate a standardized format for the information. The information could be distributed in a federated manner or contributed to a centralized repository.

  – The contributors do not provide accountholder personally identifiable information and the accounts are tokenized.
Safety and Security

S.1 Risk management

- Please describe how the individual networks’ requirements, standards, and processes will be aligned, defined, and enforced across networks to deliver a consistent risk management approach and end-user experience
  - The risk management committee from the organization governing universal sharing will define the standards that will be adopted by member networks. The committee may amend the standards periodically as deemed appropriate.
  - The risk management committee will determine prefunding standards that will be used to minimize counterparty risk. Networks will maintain the prefunding levels required for their financial institutions and for their inter-network activity.
  - Disposition of unauthorized, fraudulent, or erroneous transactions are defined in network rules and corrected using exception item processing procedures.
  - Member networks will require participating financial institutions and their service providers programs meet these standards. It will be the responsibility of the financial institutions to ensure compliance of their programs and of their affiliated service providers.
  - Networks will require member financial institutions to report periodically on their programs and to attest to their compliance with the risk management policies.
  - Networks will enforce member compliance. If unresolved, networks will take disciplinary actions to rectify non-compliance.
  - The risk management committee will require networks to periodically report their policies, procedures, and audit of participant adherence to risk management standards.
  - The risk management committee will enforce network compliance. If unresolved, the risk management committee will take disciplinary actions to rectify non-compliance.

- Please provide any details on incentives to encourage network participants to address and contain risks that they may pose to other participants.
  - The risk management committee may define a schedule of fees or other sanctions for non-compliance.
  - As a last resort, the risk management committee may refer non-compliant members to the board for removal from the sharing arrangement.
S.2 Payer authorization

- Will preauthorized payments be included in the Solution’s basic functionality? If so, how will a consistent end-user experience be assured across participating networks/FIs?
  - The solution would include the capability to perform preauthorized transactions.
  - Preauthorized payment transactions are common today in both intra-network and inter-network (“shared”) transaction sets.
  - Preauthorized payments may include both single and recurring payments.
  - The shared network rules and message specifications would define standards that would be implemented across networks.

S.3 Payment finality

- Will mechanisms be developed to support consistent revocability of payments across all participating networks/FIs?
  - Each network has existing facilities for exception item processing. Those facilities can be used by member financial institutions for shared network transactions.
  - Networks will interface their exception item processing systems with peer networks in the sharing arrangement.
  - The shared network rules and specifications will provide a unifying standard for revocability of shared network transactions.

- Will mechanisms to support disputed payments be required to meet consumer protection regulations? Will all networks have similar/identical dispute policies and processes?
  - At a minimum, the shared network rules will support regulatory and statutory consumer protection requirements.
  - Shared network rules will defined standard dispute and exception item processing requirements across participating networks.
  - Dispute policies and procedures are implemented by financial institutions and are disclosed to their accountholders. They must be in line with statute, regulation, and network rules.
  - Exception item processing policies and procedures are implemented by networks in support of the shared network rules.
S.4 Settlement approach

- Please define a path to real-time settlement for all use cases supported by the Solution.
  - Phase 3 of the proposal provides the ability for networks to override default daily settlement and perform real-time settlement.
  - Financial institutions participating using real-time settlement will authorize the network as a Fedwire Third Party Service Provider.
  - The networks will define an indicator in the transaction request that service providers may use to request real-time settlement on a transaction. Accountholder’s depository financial institution will see the indicator in the transaction request.
  - There are no differences in how networks authorize and clear transactions based on their settlement disposition.
  - If the accountholder’s depository financial institution approves the transaction, the network initiates settlement using Fedwire.
  - Networks remove transactions that were indicated for real-time settlement from their daily net settlement batches.
  - Any transaction could be eligible for real-time settlement.

S.5 Handling disputed payments

- Please describe the requirements that will be implemented to protect business and government payers as commercial transactions come on line. Will the Solution leverage/extend existing network approaches where available? How will compliance with these requirements be monitored?
  - The solution does not require specific controls applicable to business and government payers. However, as determined by service provider, configurable detective controls, such as establishing transaction limits, setting alerts, and fraud monitoring systems would be available as a method of proactively managing risk and avoiding disputes.
  - The Governing Organization will appoint a Grievance Committee. The Grievance Committee will establish a set of minimum real time payment dispute standards that will be placed upon participants. Existing industry dispute standards will be leveraged and implemented where appropriate to foster consistency across network participants.
  - Specifically, if any dispute arises between participating institutions, an earnest effort shall be made to adjust the difference, complaint, or grievance through good faith adjustments and, if necessary, negotiations between the involved parties.
S.6 Fraud information-sharing

■ How will the Solution support information sharing among providers to manage and mitigate fraud?
  – Data will be contributed by the network operators.
  – Providers of fraud detection systems may use the shared data for analytical purposes.
  – They distribute model updates and fraud trend bulletins that may be used to improve rules.

■ How will fraud information be aggregated, stored and shared?
  – Q&A for E.7 discusses two models for data sharing – centralized or federated
    □ A distributed ledger system, such as a blockchain, may be suitable for the federated model. Networks would manage nodes and contribute transaction data, including frauds that are broadcasted to other nodes.
    □ In the centralized model, the organization governing the sharing agreement would need to manage or contract management of a facility. Networks would transmit the transaction and fraud data to be added to the repository.

■ Will the Solution provide differential access to the data? How will this access be monitored?
  – No, whether a federated or centralized model, the users may access the same level of information.
  – The information will not contain personally identifiable information and account information is tokenized.

■ How will network-wide patterns be detected and anomalies shared with participants?
  – The fraud detection system providers will have access to the data to perform analytics and detect anomalies and trends. They may provide bulletins and system improvements to participants that subscribe to their services.

■ Will the Solution support real-time fraud monitoring? If so, what impact will this have on transaction speed?
  – Yes, however, the solution does not call for a centralized choke point for transaction switching or fraud monitoring. A financial institution will use its own real-time fraud monitoring system or contract it to processors or networks. Most already have such a system monitoring their transactions today.
  – From our experience, the inclusion of any real-time fraud monitoring should add less than 100 milliseconds to authorization processing.

■ Will the Solution require customer notifications and/or alerts as part of the fraud monitoring capability?
  – Financial institutions and their providers have implemented a number of alerts, such as – email, SMS, phone calls. These systems will be used at the discretion of an accountholder’s depository financial institution.
■ Will the Solution use data provided by entities other than the Solution’s providers and operators? If so, how will this third-party data be aggregated, managed, and protected? Which parties will have access to this information?

– No

S.7 Security controls

■ Please provide more information on the security controls that are currently in place at participating networks. Please provide detail about the minimum security standards and controls that would be imposed on participating networks by the risk management committee.

– Each participating financial institution, processor, merchant, independent service organization, and third-party service provider involved in authorizing, processing, or settling real time transactions or having access to real time payment information will be required to comply with real time payment security standards.

– The role of the Risk Management Committee will be to adopt a set of minimum real time payment security standards and controls to be placed upon participating networks and their participants. The Risk Management Committee will meet regularly, and existing domestic and international standards will be considered, leveraged, and implemented (e.g. Payment Card Industry) where appropriate to help foster consistency across network providers. We envision minimum security standards, including but not limited to the following areas:

□ Governing Security Policies
□ Protection of Sensitive Data (e.g. PII) in storage or in transit (e.g. encryption)
□ System Configurations
□ Application Development
□ Vulnerability/Patch Management
□ Change Management
□ User Access Controls
□ System Identification and Authentication
□ Physical Security Controls
□ Security Testing and Auditing

– Currently, most networks adhere to similar security standards, such as the Payment Card Industry Data Security Standard. These standards, as well as any forthcoming guidance from the Federal Reserve Faster Payments or Secure Payments Task Forces, will be leveraged when considering the new faster payments security standards. It should also be noted that as advances in security occur, new security controls and protocols will be evaluated by the Risk Management Committee in conjunction with existing standards and certified as appropriate for real time payment usage. Network participants will be required to utilize a third party to validate security controls annually, and submit compliance attestation with the real time payment security controls to the Risk Management Committee. To facilitate compliance with the security standards, which
are designed and required to protect the integrity of the real time system, the Governing Organization will impose fines and/or other sanctions (including possible termination) against participants (including processors and all other entities contractually obligated to comply with the security standards) for failure to comply with the requirements.

S.8 Resiliency

- Will the Solution define SLAs for participating networks related to availability? How will these be enforced?

  - Because the real time system will depend largely on third party providers to perform critical functions, the development of strong resiliency standards, including SLAs, will be necessary to ensure trust and confidence in the system. These SLAs will provide the Governing Organization the ability to identify, measure, monitor and mitigate risks with the real time system.

  - Each Participating Financial Institution, processor, merchant, independent service organization, and third-party service provider involved in authorizing, processing, or settling real time transactions will be required to comply with real time resilience standards.

  - Similar to the security standards, the role of the Risk Management Committee will be to adopt a set of minimum real time payment resiliency standards and controls that would be placed upon participating networks and their participants. Existing domestic and international standards will be considered, leveraged, and implemented (e.g. FFIEC Appendix J) where appropriate to help foster consistency across network participants. We envision minimum resiliency standards, including but not limited to the following areas:

    - Business Impact Analysis and Risk Assessment
    - Incident Management, Disaster Recovery and Business Resumption Planning
    - Business Continuity Program, to include Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for real time systems and any interdependent systems
    - Testing Policy, to include frequency of tests, outcome tracking, and monitoring of issue remediation
    - Third-party/Vendor Management Review Program

  - The committee will also develop enforcement policies to accompany the SLAs. Finally, the Risk Management Committee will be responsible for implementing governance practices to periodically audit and measure each network’s adherence to the established SLAs. To facilitate compliance with SLAs, which are designed and required to protect the integrity of the real time system, fines and/or other sanctions (including possible termination) against participants (including processors and all other entities contractually obligated to comply with the real time rules) may be imposed for failure to comply with the requirements, including the rules, technical specifications, standards and required transaction type support.
■ Please describe how the Solution will ensure that each participating network has effective business continuity and disaster recovery plans in place. How will alignment across participating networks be delivered? How will DRP and BCP be required to evolve to support the inclusion of contextual data? Real time settlement?
  – See Resiliency above

■ Please describe how the Solution will support regular contingency testing across all of the participating debit networks.
  – See Resiliency above

S.9 End-user data protection

  – See Security above

S.10 End-user/provider authentication

■ Will the Solution define minimum requirements for providers to authenticate end-users?
  – The solution does not constrain service providers on their methods of authenticating end user access to their own systems.
  – An accountholder’s depository financial institution authenticates it’s accountholders during transaction authorization.
  – The operating rules will require certain types of authentication be used in conjunction with some transaction types and may otherwise adjudicate liability based upon the type of authentication attempted and used.

■ How will participating networks be monitored to ensure industry standards for end-user authentication have been met?
  – Networks will not authenticate end users. The networks will pass authentication information (PIN, password, cryptogram) through to the accountholder’s depository financial institution for verification.

■ Please provide the process for modifying the authentication models as the threat landscape changes.
  – The risk committee may review and approve new authentication methods.
  – The network rules may be amended to state when the new methods are appropriate to use and their effect on liability.
S.11 Participation requirements

Please describe how the Solution will ensure that participating FIs and non-banks have the operational, financial, and legal capacity to fulfill their obligations (S.11.1).

- The association will establish predefined criteria used to evaluate participant soundness, such as risk weighted capital, leverage capital, broker deposit ratio, and Texas ratio.
- Networks will be required to mitigate risk with predefined prefunding deposits based on the volume and risk profile of the participating financial institutions.
- Member networks will be required to implement procedures to evaluate financial institution applicants relative to these criteria and if appropriate participants may be required to increase prefunding deposits at the network to offset risk.

Please confirm that the Solution includes processes to regularly monitor and ensure providers’ compliance with participation requirements.

- Service providers are sponsored into a network through financial institutions.
- Network participation agreements hold financial institutions responsible for their service providers’ compliance to regulations, statutes, and network rules.
- Networks may have varying policies and procedures to audit, monitor, or otherwise mitigate risks associated with service provider compliance.
- To standardize compliance regimes, including any reporting and monitoring requirements, the governance body for the sharing arrangement may create pass-through provisions that networks are required to add to their participation agreements.

Speed (Fast)

F.1 Fast approval

Please describe how transaction times may be impacted if multiple networks are involved in processing a transaction.

- Transaction times are not incrementally impacted by the proposed solution. The solution does not require transactions to use multiple networks. An additional network is only used if sharing is required because the participants are not otherwise members of the same network.
- Today, many transactions effectively already have multiple switch routing hops, where they are routed from a processor to network to a processor and then the accountholder depository financial institution. The processors are often actually other network operators that are fulfilling a “processor context” in these transactions. In sharing, technically, there will be no difference in the number of hops or processing time. Only the business arrangement is different, because the participants are not required to participate in multiple networks for commonality because the sharing arrangement suffices.
What will the approval requirement (in seconds) be for participating networks?

- Networks generally do not approve transactions, they route them to an accountholder’s depository financial institution for approval.
- If a network cannot directly route a transaction to the accountholder’s depository financial institution, then it should immediately send the transaction to the network in which the depository financial institution is a participant.
- A network should be allowed less than 1 second to route the transaction to the appropriate peer network.

If real time fraud monitoring is included in the Solution, what are the anticipated impacts on transaction time?

- Real-time fraud monitoring is in the domain of the accountholder financial institution, as part of the authorization process. It should add less than 100 milliseconds to their response time.

F.2 Fast clearing

What will the clearing requirement (in seconds) be for participating networks?

- The solution uses single message transactions for most use cases, so clearing happens at the point the accountholder’s financial institution has approved the transaction. This occurs within the example 400 millisecond full transaction cycle.

F.3 Fast availability of good funds to payee

How will the Solution support fast availability of good funds to payees in commercial transactions? Is there any requirement for providers to support and select real time settlement in order to provide available funds upon approval of the transaction?

- The networks provide the accountholder’s depository financial institution transaction codes that identify “good funds” credits.
- Operating rules will require that large commercial transfer amounts use real-time settlement for fast funds availability.

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

Please describe how the Solution will support real-time settlement options for both retail and commercial transactions as these options become available in the market.

- This is described earlier in this addendum under S.4

F.5 Prompt visibility of payment status

Does the proposer intend to require the provision of payment status notifications to end users across all participating networks to ensure a consistent end-user experience?

- The networks will not communicate with end users directly, except unless requested to do so as a value-added service on behalf of a financial institution.
– Service providers and financial institutions will communicate to their end users using channel, frequency, and detail of their choice with the constraint that it conform to applicable regulations.
– While end user experience may differ from one service provider to another, the end user experience does not differ by network or networks used for a transaction.

Legal

L.1 Legal framework

- 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 The Solution should identify relevant and applicable legal sources such as existing public sector laws, regulations, regulatory interpretations or rulings, court decisions and/or Payment System Rules that will apply to the Payment System, End Users, Providers, Payers and Payees, and payments through the Payment System.
  □ Regulation E, UCC, Durbin Amendment/Reg ii, GLBA, PCI DSS Security Standards, BSA (AML/ATF, MSB), FFIEC IT Examinations
  □ ACH operators are required to share transactions. The proposal suggests that it should be applicable to other vital payment system networks. A refusal to share transactions creates fragmentation in the payment system. It allows dominant market participants to restrict access and implement discriminatory pricing policies, ultimately harming consumers. Payment networks are an essential facility for consumers, businesses, and financial institutions. In 1912, the Supreme Court recognized bottleneck monopoly in United States v. Terminal Railroad Association. The Justice Department commented on this issue in May 1974 when an entire class of financial institutions (thrifts) were not allowed to participate equally in the payment system, saying “Antitrust law requires that those who control an essential facility must grant access to it on reasonable and non-discriminatory terms to all competitors.” After court cases and policy dialogue, the Monetary Control Act of 1980 was passed, the Federal Reserve modified pricing policy and it opened participation in the payment system to thrifts.

- L.1.2 The Solution should identify any known gaps in legal sources with respect to the proposed Legal Framework for the Solution and describe any plans to address those gaps.
  □ There are no gaps assuming industry stakeholders agree to form the governing organization and networks share transactions.
  □ Otherwise, there may be a need for a statutory mandate requiring sharing. An alternative may be expansion of the Federal Reserve Bank’s payment operations to facilitate interoperability as a network of last resort.

- L.1.3 The Solution should describe how Entities and payments through the Payment System (from Payer to Payee) will be legally bound within the proposed Legal Framework for the Solution.
  □ Financial institutions are bound through their participation agreements with the networks.
  □ Financial institutions are required to have agreements with their service providers and accountholders that articulate their rights and responsibilities.
L.1.4 The Solution should describe how it supports compliance with relevant U.S. law by all End Users and Providers when sending and receiving payments. U.S. law includes OFAC, AML, BSA, the UIGEA (Regulation GG), Federal Consumer protection regulations (such as Regulation E and Regulation Z), Federal and State MSB laws, and all other applicable Federal and State laws.

- Network participation agreements hold financial institutions responsible for compliance of their programs with all applicable regulations and statutes. They are responsible for the activities of their service providers.

L.1.5 The Solution should identify any unique legal provisions needed in the Solution’s Legal Framework to address any situations in which End Users/Providers will perform the same functions in the Payment System, but are subject to different applicable U.S. banking and payment laws and/or regulatory supervision.

- If an end user assumes a service provider capacity, the financial institution will need to ensure the end user has accepted terms and conditions from a service provider agreement.
- If service provider assumes an end user capacity, the financial institution will need to ensure the end user has accepted terms and conditions from an end user agreement.

L.2 Payment system rules

■ 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 The Solution should describe key features of existing or proposed Payment System Rules governing the rights and obligations of all End Users, Providers, Payers and Payees to enable the Payment System to operate effectively and efficiently, including Payment System Rules addressing:
  
  L.2.1.1 Authentication of all Entities, payments or messages connected to a payment;

  - Transactions are entered into the network through a participating financial institution or a service provider that is sponsored by a participating financial institution. Networks board service providers, financial institutions (and their processors) and provide them keys that are used for authentication of their communications.
  
  - Service providers may authenticate end users with any number of proprietary means before allowing them to initiate a transaction.
  
  - In some cases, service providers may collect authentication information (PIN, password, cryptogram) that is passed through the network to an accountholder’s depository financial institution for verification.

  L.2.1.2 Legal responsibility of Providers that provide Payment System access to End Users;

  - Network rules require service providers to have an agreement with a participating financial institution.
  
  - The financial institution agreements with their service providers require the service providers to comply with all network rules, regulations, and statutes.
- **L.2.1.3 Payment Order Initiation/Authorization and termination of Authorization;**
  - With single message transactions, the authorization and financial clearing are conducted at the same time. The order cannot be terminated once sent. A good faith adjustment may be requested if the payment order was sent in error.
  - With a dual message transaction, the service provider may reverse and authorization.

- **L.2.1.4 Cancellation of a Payment;**
  - Payments are final once approved. Good faith adjustments may be requested.

- **L.2.1.5 Delayed and failed payments;**
  - The solution uses real-time authorization and clearing. If a payment is not approved within the required timeframe, it is reversed to resolve ambiguity. The service provider may then re-initiate.

- **L.2.1.6 Payment Finality and Settlement;**
  - Transaction payment is final when authorized and cleared.
  - Timing of settlement is communicated from the network to its participating financial institutions. If real-time settlement is requested by a service provider, the participating financial institutions will be made aware through an indicator in the transaction.

- **L.2.1.7 Timing of sending and receipt of a payment;**
  - The transactions are real-time. The payment is received when the accountholder’s depository financial institution receives the transaction and provides a response to the network.
  - Network rules specify the maximum allowable time for the accountholder’s depository financial institution to respond to the authorization or clearing request.
  - The members will need to agree on a maximum allowed response time in the rules. We propose no more than 2 seconds.

- **L.2.1.8 Records as proof of payment for Payers and Payees; and**
  - Transactions are posted to accounts at the depository financial institutions.
  - Accountholder depository financial institution record retention requirement of at least two years.
  - Network retains transaction history for research for the duration of the allowable dispute period.

- **L.2.1.9 Error Resolution for anticipated disputed payments (see S.5) among End Users, Providers, Payers and Payees.**
  - End users dispute payments through their depository financial institutions. Consumers enjoy Regulation E protection from unauthorized transactions.
  - Credit payments are to be treated as good funds, so the payer may only request a good faith adjustment.
  - Debit transactions may be adjusted back to the originator if network rules provide liability protection for the accountholder’s depository financial institution.
L.2.2 If different than the process set forth in G.1 and G.2, the Solution should describe the process that was or will be used for the development and amendment of the Payment System Rules, including the process for obtaining input from Payment System stakeholders.

- Refer to G.1 and G.2

L.2.3 If different than the process set forth in G.1 and G.2, the Solution should describe how Payment System Rules will be enforced and monitored, including whether or not an organization or regulators may enforce the rules.

- Refer to G.1 and G.2

L.2.4 The Solution should describe existing or proposed Payment System Rules for allocating legal responsibility to appropriate Entities to obtain valid Authorization from the Payer.

- Financial institutions that sponsor service providers are accountable for activity submitted into the network by their service providers. They are required to have agreements with their service providers. These agreements require service providers to obtain authorization from payer end users.

L.2.5 The Solution should describe existing or proposed Payment System Rules related to an Error Resolution process within the Payment System for End Users and Providers to correct or otherwise resolve errors, unauthorized transactions or disputes in the payment process (see also S.5 and L.3).

- Accountholders dispute according to Regulation E (consumer) or otherwise terms and conditions provided by the financial institution. The network rules may provide for additional coverage that is added to accountholder terms and conditions with their depository financial institutions.

- We have described this in sections U.3 and S.3.

L.3 Consumer protections

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 The Solution should describe a Legal Framework for allocating legal and financial responsibility for all Entities for losses in the event of a Payer or Payee claim of unauthorized, fraudulent or erroneous Consumer payments.

- Consumers are protected by Regulation E, and they dispute transactions with their depository financial institutions.

- Network agreements with participating financial institutions hold them accountable for their end users’ (service providers and accountholders) transaction activity and any losses associated with unauthorized, fraudulent, or erroneous payments.
L.3.2 The Solution should establish Payment System Rules and procedures that support Error Resolution for Consumer claims arising from payments Fraud, unauthorized payments or errors.

- Network agreements and operating rules require participating financial institutions to provide consumer protection from unauthorized transactions, to disclose their rights to consumers, and to provide consumers dispute procedures.

L.3.3 The Solution should include option(s) for End Users, Providers and/or the Payment System to establish additional Consumer protections for payments, which may exceed those protections that are otherwise required under applicable law.

- Many networks have rules that require additional protection above the minimum required by Regulation E. The universal sharing agreement will require participants to provide 100% protection to the consumer to ensure a standard experience.
- Protections for service provider and commercial accounts will be dictated by the terms and conditions of their agreements with their financial institutions.

L.4 Data privacy

L.4: Please provide more details regarding data privacy, including an approach to identify whether and how payment and related information can be collected and disclosed, consistent with applicable policy, law, and End User preference, and an approach, consistent with law, to secure information that should not be disclosed. In doing so, please specifically address how the Solution supports the five data privacy subcriteria.

L.4.1 The Solution should describe its approach to Data privacy and Confidentiality of payment and related Data. For example, the Legal Framework should describe limitations on End Users’ or Providers’ collection of Data and use or disclosure of payment Data to third Parties.

L.4.2 The Solution should describe its approach to Data security of payment and related Data, taking into consideration the application of legal requirements. For example, the Legal Framework should describe operational procedures and policies to secure Data within the Payment System and at End-User and Provider locations.

L.4.3 The Solution should describe the nature and type of End-User Data that may be required for security, legal compliance and Authentication purposes within the Solution.

L.4.4 The Solution should describe how End Users may get visibility into the Data being collected on them, limit sharing of such Data, and change their privacy preferences with regard to proposed uses of End-User Data.

L.4.5 The Solution should describe its approach to Data breaches at the Payment System or at an End User/Provider, the responsibilities (including notifications) of the End Users/Providers in the event of such a breach, and whether the Legal Framework seeks to allocate financial or other responsibility among End Users and Providers in the event of a Data breach.
L.5 Intellectual property

- 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.

  - L.5.1 The Solution should set forth a proposed approach for the Payment System, End Users and Providers to resolve or manage, prior to implementation, any legal, operational or financial risks arising from third-party intellectual property rights (including patents, trademarks, copyrights and trade secrets). This proposed approach should include whether or not the Solution has undertaken or will undertake a due diligence review of potentially applicable intellectual property rights.

    - When members join the association, they will agree that any contributions to will become property of the not-for-profit association unless otherwise declared as restricted, intellectual property.
    - In creating solutions that conform to the governance body’s rules, processors, networks, and other stakeholders may of course develop or license proprietary solutions.

Governance

G.1 Effective 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.

  - G.1.2 The Solution’s governance arrangements should be publicly disclosed.
    - For purposes of accountability and transparency the bylaws will be made publicly available.

  - G.1.3 The Solution’s governance arrangements should provide a process to handle appeals related to specific decisions or their implementation.
    - Members may appeal and the board reconsider decisions.
    - The board may form an appeals or grievances committee or allow other standing committees to field appeals within their jurisdictions.

  - G.1.4 The Solution’s governance arrangements should provide for independent validation of compliance with the Solution's rules, compliance with applicable law, and achievement of both the Solution’s objectives and public policy objectives.
    - The organization will hire an independent auditor to review its operations.
    - The audit results will be reviewed by management and the board of directors.
G.2 Inclusive governance

■ 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.

– G.2.1 The Solution’s governance arrangements should include consideration of the public interest when making decisions and rules.
  □ The governance body will reserve board seats for public sector representatives.

– G.2.2 The Solution’s governance arrangements should provide for input and influence by all stakeholders, through one or more governance or advisory bodies.
  □ All stakeholder classes will be assured equal representation in committees and working groups.
  □ Request for comment process will allow stakeholders that do not directly serve in the groups to provide input for consideration by their representatives.

– G.2.3 The Solution should have governance and advisory bodies that fairly represent stakeholders’ interests and risks.
  □ Work groups and standing committees would be organized from among the membership. Ad hoc work groups may be created for special initiatives. Standing committees with rotating memberships would be required for rules, pricing, risk, and specifications.
  □ The organization’s bylaws will need to ensure that the rotations provide classes of stakeholder equal opportunity for representation in the committees.

– G.2.4 The Solution’s governance approach should enable specific stakeholders or stakeholder groups to proportionately influence outcomes.
  □ The proposal seeks to provide an environment fostering equal and non-discriminatory access to the payment system. All stakeholders have an interest in the payment system; however, proportional influence accrues unfair advantage to incumbent networks and relatively large financial institutions.
  □ The governance organization for universal sharing would have a limited stock ownership structure or otherwise define its voting rights in a manner that ensures equal representation and control by all classes of stakeholders.

– G.2.5 The Solution’s governance approach should address and manage actual, perceived, or potential conflicts of interest.
  □ Bylaws will require recusal when a committee decision directly affects the member – for example, a member should not participate in a committee vote to sanction the member.
Faster Payments QIAT

DRAFT ASSESSMENT

Proposer: SHAZAM, Inc.

Summary Description of Solution

The solution is less a technical proposal than it is a case for the universal sharing of information and equitable participation among the existing debit networks. It seeks a broader definition of "network": in Shazam’s view, not only debit networks should be considered to be “networks”; any two or more financial institutions (FIs) that directly exchange transactions should also be redefined as “networks.” These FI networks, then, should be required to share information with other networks just as ACH operators are required by NACHA to share transactions.

The proposal focuses primarily on developing a governance model for sharing information among these broadly defined networks. “Sharing information” is defined as one “payment brand [i.e., network] facilitating a transaction into another payment brand” (page 6). Shazam maintains that requiring information-sharing would address the “payment brand participation gap” and achieve functional interoperability among debit networks.

Based on this premise, the solution facilitates debits and credits to a deposit account in real time using a real or tokenized account identifier. The solution relies on existing network rules, processes, and procedures related to clearing and settlement. The solution addresses the network aspect only, and responsibility for end-user requirements related to authentication, access channels, disputes, etc. will belong to the connecting providers.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths

— The solution proposes a governance framework for competing networks based on the requirement to "share information" that the proposer believes will facilitate sharing and thus interoperability among debit networks.

— By leveraging existing debit network infrastructure, processes, and capabilities, the solution allows for ubiquitous end-user access, either through a participating FI or through a regulated, non-financial institution holding a master account at a participating FI. The proposal does not depend on any new directory capabilities, but suggests that payment account token prefixes continue to be used to route transactions, networks continue to exchange directories and new concepts can be introduced that extend existing directories.

— Individual service providers can determine which alias(es) (e.g., cell phone number, email address, etc.) they wish to support for payment and can connect the alias information to the payment account token.

■ Areas for improvement and enhancement

— The solution calls for mandatory interoperability among debit card networks. Most specifications will be provided by the existing card networks, and sharing rules would be developed and maintained by a future governance body such as NACHA, the Federal Reserve Bank or a new, not-for-profit rules-making organization. The solution calls for the use of a system that is readily available today, and that does not modify the payment process or experience to deliver faster
payments or new use cases. Rather, it merely increases the reach of current solutions built on a single network.

- The solution relies on existing debit network policies and procedures to support all stages of the transaction, including clearing and settlement. Each network would continue to operate as it does today, but would support the routing and transmission of additional, “out of network” transactions. It also depends on a token to drive the alias, but it does not describe how tokens other than card numbers would be created, nor does it describe where this information would be made available to network participants.

- The solution leverages existing settlement solutions and calls for the use of prefunding or FedWire for settlement of urgent payments. The solution makes no mention of connecting to TCH (The Clearinghouse) and other real time capability once available in market. At its heart, this proposal seems to be a request for a regulatory requirement that would force networks to share transactions.

- The solution is much less a technical solution than it is about governance. As is, the solution does not advance the payment system broadly, but rather focuses on making it easier for debit networks to compete with "direct-connect" banks. The solution has a five-year implementation timeline with a general framework for how rules would be built, but the proposal lacks specifics.

- **Use cases addressed**

  - The solution is not applicable to all use cases. Major elements are missing (e.g., remittance sharing) for specific use cases, such as B2B. If all described upgrades are executed, the solution’s technical design will support all use cases over time.

  - Phase I lasts for two years and focuses on the creation of governance rules. Phase II lasts for one year, and calls for the delivery of ‘basic functionality’: P2P (person to person) and B2P (business to person) use cases. Phase III lasts for one year and calls for the introduction of B2B (business to business) and P2B (person to business). The delay in delivering any use case in the first two years is due to the need first to design a governance plan and then to determine how to support interoperability.

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

  - This proposal is high-level and requires a substantial change in the debit networks’ operating models in order to be successful. To effect the change the proposer is seeking, the definition of “network” must be fundamentally changes to include direct-connect banks. If the requirement to share transactions is delivered, smaller networks such as Shazam could compete more effectively against larger networks, as the value of scale would be diminished. This level of ubiquity for information sharing is likely to be achieved only via mandate.
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 proposal’s objective is to eliminate “fragmentation [of] and discriminatory access” to the payment system. To accomplish this goal, all networks must participate in the system. The proposer does support the notion that a valid business case may exist for certain direct-connection relationships to remain intact.

As proposed, the solution and its accessibility rely entirely on the mandated sharing of transactions and full adherence to existing debit network rules. To enable interoperability (U.1.6) among participating networks, a new rules-making organization will need to be created to develop a common set of rules. The proposal sets forth a high-level, five-year implementation plan to create its industry-level governance model (U.1.5); the first two years of the plan are focused on aligning participating networks through the creation of solution governance.

The solution facilitates payments to and from accounts that can be linked to a debit network (U.1.1). At launch, the solution considers only retail accounts, with commercial accounts to be added in a later phase. Any regulated, non-bank PSP (payment services provider) can have access to the solution as long as it holds a master account at a participating FI (U.1.1), thereby providing access to the unbanked (U.1.4).

However, the solution does not initially support payments to and from all end-user accounts (U.1.2). The proposer can strengthen the proposal by detailing a clear plan to accelerate specific, unmet use cases such as P2P and B2P. For example, in the current proposal, those use cases will be supported in Year 3 of the implementation plan, while B2B and P2B are part of Phase III deployment in Year 5. Accelerating the inclusion of those use cases could enhance the proposal’s viability. It could be further improved by providing a clear plan showing how international cross-border payments will be enabled through a collection of domestic debit networks, as these networks only operate in USD.

U.2 Usability

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

**Rationale:**

The solution is available to users 24x7x365 through a variety of devices and channels (U.2.1, U.2.3). For authentication, the solution supports the use of tokenized account information (U.2.2), but it is not clear which alias options (e.g., email address, cell phone number, etc.) will be supported across participating networks to ensure consistency. The solution’s authentication role in relation to the individual networks is likewise unclear, although the proposal does state that service providers are responsible for authentication (page 10).
While the solution is device- and channel agnostic (U.2.1), and the transactions set for universal sharing should include all transaction types, the governance body needs to define which transaction types are mandatory for the solution.

Much of the end-user’s experience is the provider’s responsibility and will be subject to existing debit network requirements and, potentially, inter-network requirements. As a result, the customer experience could vary from network to network (U.2.3). The proposal could be enhanced by explaining how some of this potential variability could be avoided by establishing a set of minimum standards in the network participation and operating rules. Additionally, payment system rules regarding notifications need to be developed to require and enable payment status notifications to payees (U.2.4).

**U.3 Predictability**

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

**Rationale:**

The solution relies heavily on existing debit network rules, requirements, and processes, and it is unclear whether these requirements and processes can be aligned across networks to ensure predictability. The solution is channel- and device-agnostic, as service providers determine which devices and channels are acceptable, with limited constraint by network rules or applicable regulations. Essentially, this flexibility facilitates competition by allowing service providers to differentiate end-users’ experience.

To facilitate a consistent experience for end-users’ interactions with each other and other parties (U.3.3), the solution leverages ISO8583, a legacy messaging format common among debit and ATM networks that is not used broadly beyond POS and ATM transactions. The proposal contemplates the use of translation engines for various “dialects” (each network’s particular implementation of ISO8583) (page 11). The proposal could be strengthened by detailing a plan to support the emerging ISO20022 messaging standard rather than taking a “wait-and-see” approach (page 11).

**U.4 Contextual data capability**

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

**Rationale**

The solution’s standard messaging format is ISO8583, a legacy format that, in its current iteration, does not support the transmission of contextual data. Without the use of ISO20022 or an expanded translation capability, the solution cannot provide detailed remittance data. The proposal does discuss adding support for contextual data, but the capability will not be introduced until Phase 3, in conjunction with commercial use cases B2B and P2B.

The solution could be enhanced by introducing contextual data capability into an earlier phase, likely Phase 2, given the current implementation timeline. (Phase 1 is the two-year governance phase, while Phase 2 is a one-year effort to build basic interoperability.) The proposal suggests that payees could access remittance data through a URL (page 14) or QR code (page 16) associated with the transaction; the proposal could be strengthened by providing details about the specific
information that will be provided in the URL or QR code and describing how the URL or QR code will be transmitted i.e., via ISO8583 or another communication channel).

**U.5 Cross-border functionality**

<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 could be strengthened by clarifying how the solution would enable convenient, cost-effective, timely, secure, and legal payments from other countries (U.5.1). The proposal indicates that some of the participating debit networks would support international transactions, but it needs to explain how the solution itself will support those transactions (U.5.2). To strengthen the proposal, it would be helpful to discuss which networks will participate, which networks have cross-border functionality, and how cross-border functionality can be extended to end-users of other debit networks. The inclusion of cross-border transactions is currently slated for Phase 2; the proposal could be enhanced by detailing how this capability will be added (U.5.5).

**U.6 Applicability to multiple use cases**

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

**Rationale:**
According to Shazam’s five-year implementation plan, the solution will support the main use cases, but not immediately. The first two years (Phase 1) will be spent designing a governance plan; the following year (Phase 2) will be spent building basic interoperability. This second phase will support the P2P and B2P use cases. In Phase 3, the “commercial enablement” phase, the solution will enable B2B and P2B payments and will add ISO20022 capability to support remittance information. As mentioned above, the solution could benefit from accelerating the phases of its implementation plan.

**Efficiency**

**E.1 Enables competition**

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

**Rationale:**
The solution would create a single large network consisting of multiple debit network providers; it thus could potentially increase the number of networks a participating FI could leverage (E.1.2) and would benefit smaller networks that have less reach and functionality than their larger counterparts. In theory, an FI could have a relationship with any debit network provider and have access to all of the features and functionality of the largest network (E.1.4). FIs will likely be able to choose the lowest-cost provider and to switch between providers without losing core functionality (E.1.1-2). Responsibility for cost disclosures is left to participating FIs (E.1.3).
As discussed in previous criteria, however, the solution relies on existing debit network requirements, rules, and regulations. The proposal could be enhanced by explaining how requirements, rules, and regulations will be aligned across the participating networks (E.1.3 and E.1.4).

E.2 **Capability to enable value-added services**

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

**Rationale:**
Providers can develop value-added services, but such services fall outside of the solution’s immediate scope. Individual networks will develop new products and services beyond the solution’s core functionality to differentiate themselves enough to win direct connection, just as they do today. While this approach could facilitate differentiated functionality and end-user experiences, the ability to introduce new functionality may be limited, given that ISO20022 will not be available until Phase 3 of the solution. Successful implementation of the solution will allow service providers to choose among a greater number of networks that can provide universal access.

The proposal can be enhanced by discussing how providers can integrate with the solution via open and accessible standards to offer value added services (E.2.1) and how all providers can offer value added services as long as they adhere to a minimum set of participation requirements (E.2.2).

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:**
As mentioned, the proposal describes a five-year timeline divided into three phases. The first two years of implementation are focused on designing governance rather than on introducing new capabilities into the market. The proposal could be enhanced by indicating which entity will lead this exercise and maintain the documentation once created.

Phase 2 will leverage existing debit network capabilities to deliver basic functionality (B2P and P2P) within 12 months. Commercial transactions (B2B, P2B) will be delivered in Phase 3 (years 4 and 5).

The solution’s value proposition could be enhanced by accelerating the enablement of use cases (B2B and P2B, for example) and the capabilities required (e.g., contextual data) to support those use cases.
E.4 Payment format standards

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

**Rationale:**

The solution uses the ISO8583 format to start, with the use of a translation engine to address dialects (individual networks’ particular implementations of ISO8583) across networks and to serve as a bridge to the possible adoption of ISO20022 in the future. Given that ISO20022 is evolving into a de facto standard capable of supporting expanded contextual data, the Proposal would do well to develop a plan to implement ISO20022 rather than postponing this implementation until “business needs dictate” it (page 11) (E.4.4).

ISO20022 support is necessary to enable international interoperability and to support the inclusion of contextual data in relevant B2B use cases (E.4.1); a more definitive plan to support ISO20022 would thus be helpful. ISO8583, however, is interoperable for cross-border transactions among card networks with cross-border capability (E.4.2). Since debit networks already use ISO8583, message format implementation costs will not come into play until (if) ISO20022 is implemented (E.4.3). The ISO8583 message format will be updated through the ISO system (E.4.4).

E.5 Comprehensiveness

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

**Rationale:**

The solution focuses on providing network capabilities. In concert with FIs, which are responsible for the other aspects of the end-to-end payment process, it 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). To execute the payment process, the solution relies on the debit networks’ existing capabilities and their requirements of participating FIs for initiation, authorization and authentication, clearing, and receipt of transactions.

E.6 Scalability and adaptability

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

**Rationale:**

The solution’s technical design does not support all use cases at the outset, but the B2B and P2B use cases will be supported in the future (Phase 3) (E.6.1).

The solution leverages existing debit networks’ infrastructure, policies, and procedures. While the proposal does not explicitly describe how the individual networks will scale and adapt to support increased volume and new transaction types, it does suggest that latent capacity in the networks can handle any potential network scale issues (E.6.2). The proposal could be strengthened by providing transaction volume forecasts and likely processing or throughput rates (E.6.2). The proposal describes how the debit networks will adapt to ongoing developments (e.g., technological, economic developments) (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 proposal relies on individual network capabilities, rules, policies, and procedures to manage exceptions and disputes.

The proposal can be strengthened by describing how these individual network capabilities will be aligned to provide a consistent end-user experience across the solution’s core functionality and the transactions enabled by the solution and addressing the aggregation of data or monitoring of transactions for suspicious patterns at the centralized level (E.7.3). The assumption is that the participating debit networks would monitor transactions at a network level, as they do today. Once written, the solution will have a universal sharing agreement that is expected to have rules that networks must adhere to participate; it is expected that the rules will normalize the end-user experience to an extent. The proposal suggests that a federated consortium model or a centralized model is possible (page 21), but no guidelines or requirements are provided. The Proposal could be enhanced by detailing the need for a set of minimum core standards that all member networks must adhere to for handling exceptions in the solution’s operating and participation rules.

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:**

Shazam proposes creating a risk committee to develop an inter-network risk management framework that would leverage individual debit networks’ existing compliance and risk management functions. The risk management committee would serve as part of the solution’s overall governance. As such, it would monitor systemic risk issues associated with the sharing of transaction information, including counter-party risk, business continuity standards, and inter-network fraud reporting. It is not described how the individual networks’ requirements, standards, and processes would be aligned, defined, and enforced across networks to deliver a consistent risk management approach and end-user experience.

The solution places responsibility for much of the necessary risk management onto participating FIs. Risks related to settlement (S.1.2); operations (S.1.3); and unauthorized, fraudulent, or erroneous payments (S.1.4) will be addressed by the risk management committee; however, the risk management committee is not yet in place (S.1.1). The proposal could be enhanced by addressing how operators and providers will manage the risk they may pose to other participants (S.1.5) and how the risk management committee will embark on reviewing and updating the risk management framework (S.1.6).
S.2  **Payer authorization**

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

**Rationale:**

The solution leverages the authentication and good-funds authorization practices currently required by participating debit networks. The onus for payer authorization is placed directly on participating FIs, as per network participation requirements. The solution can handle pre-authorized transactions in both single and recurring payment scenarios. The shared network rules and message specifications are in place to ensure a consistent minimum standard across networks for these payments (S.2.2-3).

S.3  **Payment finality**

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

**Rationale:**

The solution leverages debit networks’ existing capabilities, functionality, and requirements for payments finality, and debit networks require that all payments be authorized to ensure good funds (S.3.1). The shared network rules, while not yet written, should provide a unifying standard for revocability of shared network transactions. The proposal indicates that the rules committee could leverage existing network rules addressing liability, error resolution, adjustments and disputes to create a consensus-driven, normalized set of rules for participants in the universal sharing arrangement (S.3.2-3).

S.4  **Settlement approach**

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

**Rationale:**

The solution will leverage existing settlement processes and the risk management activities required by participating debit networks (S.4.1). Payments will be settled in central bank funds (S.4.3). To settle transactions in the use cases that will be implemented in Phase 2 (B2P and P2P), the solution will use ACH or wire transfers. For the commercial payment use cases that will be supported in Phase 3 (B2B and P2B), the solution will evolve to accommodate real-time settlement. Phase 3 of the implementation timeline suggests that networks will be able to override default daily settlement and to execute real-time settlement instead. The proposal could be enhanced by clearly describing how real-time settlement will be implemented.

The proposal could be further strengthened by adding rules for managing credit and liquidity risks across the solution and relying less on existing network practices (S.4.2). The proposal states that the solution’s risk management committee will “define safety and soundness policies ensuring [that] networks participating in the inter-network sharing are protected from counter-party risks” (page 31).
S.5 Handling disputed payments

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

**Rationale:**
The solution will leverage existing debit network rules, policies, and procedures for handling payment disputes (S.5.1). The solution does not require specific controls applicable to business and government payers, but it does allow for configurable controls, such as transaction limits, alerts, and a fraud monitoring system. Additionally, the solution’s governing organization will appoint a grievance committee responsible for establishing a set of minimum real-time-payment dispute standards for solution participants.

The Proposal could be improved by describing how debit network participants already comply with consumer protection laws (S.5.2, S.5.5) and by listing the mechanisms in place to address disputes (S.5.3). The proposal could further be enhanced by anticipating how dispute processes will have to evolve as commercial payment use cases (B2B, P2B) are implemented (S.5.4).

S.6 Fraud information-sharing

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

**Rationale:**
The proposal considers adopting a centralized or federated approach to sharing fraud information (page 21) (S.6.1). The proposed rules-making association will define this approach. While still conceptual, the proposal suggests that a distributed ledger system may be suitable for the federated model where networks would manage nodes and contribute transactional data. The organization governing the sharing agreement will need to manage or to contract management of a facility for the centralized model. In either model, access to data will be universal and undifferentiated. The solution does support real-time fraud monitoring, but the monitoring will be executed by individual FIs. This real-time monitoring is expected to add less than 100 milliseconds to the authorizing process.

The proposal could be enhanced by establishing a set of decisions that would provide clear guidelines for adopting either the centralized or federated model for sharing fraud information (S.6.1). It can be further strengthened by creating operating rules that provide differential access to data based on roles and responsibilities (S.6.5). Providing functionality to aggregate fraud information to identify patterns can prove to bolster the solution (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 solution includes the creation of a new risk governance structure that would harmonize participating networks’ security controls and policies and then define and set standards for inter-network sharing (S.7.3). The framework that has been described, while not yet up and running, clearly sets forth minimum security standards, including governing security policies, protection of...
sensitive data, systems configurations, application development, vulnerability, change management, user access, system identification and authentication, physical security, and security testing and auditing.

S.8 Resiliency

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

**Rationale:**

The solution will leverage participating networks’ existing business continuity plans (BCPs) (S.8.2), which are regularly updated and tested (S.8.5). As with the solution’s security standards, the Risk Management Committee will need to adopt a set of minimum real-time-payment resiliency standards. The proposal could be enhanced by detailing how the current BCPs work and defining a standard approach to resiliency across the solution. It can be further improved by addressing the impact that volume increases or the addition of new transactions or services (e.g., contextual data) might have on existing BCPs.

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 debit networks participating in the solution will use payment account tokens and will not require account information or PII (personally identifiable information) to be transmitted along with transactions (S.9.3). All service providers, processors, and networks must comply with GLBA (Gramm-Leach-Bliley Act) and PCI (Payment Card Industry) requirements (S.9.1). Individual participants will manage proprietary directories to support the use of alias information (e.g., email address, cell phone number) (S.9.2). Additionally, any forthcoming guidance from either the Faster Payments or Secure Payments Task Forces will be leveraged when building additional rules for end-user data protection.

The proposal could be strengthened by clarifying how the use of aliases and access to PII stored in directories will align across networks (S.9.1 and S.9.3). It would be helpful for the proposer explain the networks’ and participating FIs’ roles and responsibilities regarding data protection.

S.10 End-user/provider authentication

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

**Rationale:**

The solution will leverage existing debit network rules for authentication (S.10.1); these rules align with regulatory guidance and industry standards for end-user authentication (S.10.3). Operating rules will require certain types of authentication be used in conjunction with some transaction types and may otherwise adjudicate liability based upon the type of authentication attempted and used.
Service providers and FIs have the flexibility to adopt authentication methods that suit their use cases and risk tolerance.

The proposal could be strengthened by addressing how the network will ensure that payments reach the intended payee or account (S.10.2), whether strong authentication controls would be applied across all channels (S.10.3), and how authentication models may be changed in response to an evolving threat landscape (S.10.6).

S.11 Participation requirements

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

**Rationale:**

The solution leverages existing debit network participation requirements, but also defines how the association will establish predefined criteria to evaluate participant soundness (e.g., risk-weighted capital, broker deposit ratio, etc.). Member networks will be required to implement procedures to evaluate FI applicants against the developed criteria.

The proposal could be enhanced by detailing how the solution will ensure that participating FIs and non-banks have the operational, financial, and legal capacity to fulfill their obligations (S.11.2)

**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 majority of Shazam’s transactions are executed end-to-end (E2E) in 400 milliseconds, and transaction approvals take milliseconds. Clearing and approval occur simultaneously. Assuming that participating FIs will comply with existing network speed requirements for providing transaction approval, the solution needs less than one second to route the transaction.

F.2 Fast clearing

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

**Rationale:**

The solution enables fast clearing, as the majority of Shazam’s transactions are executed E2E in 400 milliseconds, and transaction approval takes milliseconds. The solution’s single message format allows posting to occur simultaneously with authorization.
F.3  Fast availability of good funds to payee

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

**Rationale:**
According to the proposal, debit network rules require full funds availability upon receipt of approval. The solution’s baseline features facilitate real-time delivery of guaranteed good funds from payer to recipient. The recipient FI can decide to make funds fully available to the recipient at that point, even though settlement does not occur in real time.

The proposal suggests that operating rules will require large commercial funds transfers to use real-time settlement for fast funds availability. The proposal could be augmented by defining the amount that constitutes a “large” commercial transfer.

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

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

**Rationale**
The solution leverages settlement capabilities that are already in the market (Fedwire, ACH). In Phase 3, originators will be able to request real-time settlement on a transaction, although real-time settlement will not be required.

The proposal could be strengthened by explaining how credit or liquidity risks arising from settlement lags will be addressed (F.4.1). Further, it would be beneficial to address special considerations for settlement among providers in different time zones (F.4.2). The proposer should also consider describing how the introduction of same-day ACH settlement will affect the availability of good funds and inter-network risk management.

F.5  Prompt visibility of payment status

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
Participating debit networks will support prompt visibility of payment status. It is up to FIs to decide whether to provide notification to end-users.
Legal

L.1 Legal framework

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

Rationale:

The proposal calls for the use of existing network rules and compliance functions but does not provide any details of existing requirements. The proposal does not identify any new requirements that may be required to deliver alignment across participating networks, or to support real time settlement in Phase 3. The proposal can be enhanced by clearly describing how the rules will be aligned across all participating networks, and how minimum requirements will be determined. It is suggested that a legal framework will be developed for the inter-network solution.

The proposal acknowledges a need for a Legal Framework and sets out a fairly detailed plan to complete it, 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 “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:

The proposal states that existing network rules from incumbent networks address the issues delineated in L.2.1 and details the rules for end-users, providers, payers, and payees across a broad spectrum of payments functionality. The proposal could be enhanced by describing how minimum requirements for payment system rules will fill any gaps in existing network rules and ensure alignment across networks.

The proposal acknowledges a need for payment system rules and sets out a path to complete them, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Effective.”

L.3 Consumer protections

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

Rationale:

The solution leverages existing payment network requirements to support consumers. The proposal could be made more robust by addressing inter-network error resolution rules and procedures (L.3.2). It could be further enhanced by discussing whether end-users, providers, or the payment system may establish consumer protections for payments that augment current consumer protection laws (L.3.3). Further clarifying how requirements will be aligned across network participants to ensure a consistent consumer experience would likewise benefit the overall proposal.

The proposal acknowledges a need for consumer protections and sets out a path to complete them, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Effective.”
L.4 Data privacy

Very Effective        Effective        Somewhat Effective       Not Effective

Rationale:  
The proposal does not directly address data privacy. The solution proposes to leverage and align existing network requirements related to data privacy, but no details of these requirements are provided in the proposal. The proposal can be strengthened by describing how requirements will be applied consistently across participating networks.

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

L.5 Intellectual property

Very Effective        Effective        Somewhat Effective       Not Effective

Rationale:  
Members must agree that contributions to the association are the property of the association. In the participation rules, members agree that any contributions they make after joining the association will be property of the association unless it is declared as restricted, intellectual property (L.5.1).

The proposal can be strengthened by discussing any due diligence reviews that have been undertaken or will be undertaken to assess potentially applicable intellectual property rights (L.5.1)

Governance

G.1 Effective governance

Very Effective        Effective        Somewhat Effective       Not Effective

Rationale:  
The proposal suggests creating a new, not-for-profit membership organization with rule-making authority to provide governance for the solution. Representatives would be selected from industry stakeholder organizations. The development of the governance model will take place in Phase 1 of the solution and is expected to take up to two years. High-level elements of the model have been identified (e.g., publicly available bylaws, the ability of members to appeal decisions, the formation of an appeals or grievance committee, plans to hire an independent auditor, etc.)

The proposal could be improved by describing how decisions and rule-making would take place (G.1.1), how appeals and escalations would be handled (G.1.3), and how independent validation of compliance would be assured.

The proposal acknowledges a need for effective governance and sets out a path to complete governance arrangements, but these arrangements are not yet complete. The QIAT has interpreted
the Effectiveness Criteria such that solutions at this stage of development earn a rating of “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:**

Diverse stakeholders/participants will have input and voting rights on important issues such as rules, pricing, and specifications (G.2.2). Board seats will be reserved for public-sector representatives as part of the governance model (G.2.1). All stakeholder classes will be equally represented in committees and working groups (G.2.2-3). The proposer notes that the bylaws should ensure that board rotations allow categories of stakeholders equal opportunity for representation in committees. The bylaws will further require recusal from a committee when a decision directly affects that member (G.2.5).

The proposal acknowledges a need for inclusive governance and sets out a clear path to complete these governance arrangements, 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 “Effective.”
## APPENDIX A: ASSESSMENT SUMMARY

<table>
<thead>
<tr>
<th>UBIQUITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.1: Accessibility</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2: Usability</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.3: Predictability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.4: Contextual data capability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.5: Cross-border functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.6: Multiple use case applicability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EFFICIENCY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1: Enables competition</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2: Capability to add value-added services</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>E.3: Implementation timeline</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.4: Payment format standards</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.5: Comprehensive</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>E.6: Scalability and adaptability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.7: Exceptions and investigations process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAFETY AND SECURITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAFETY AND SECURITY (cont’d)</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td>✓</td>
<td>{o}</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>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPEED (FAST)</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>F.1: Fast approval</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>✓</td>
<td>{o}</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>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEGAL</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>L.1: Legal framework</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>✓</td>
<td>{o}</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>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOVERNANCE</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>G.1: Effective governance</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td>✓</td>
<td>{o}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

SHAZAM is pleased to have had the opportunity to present this proposal, and we are thankful for the effort put forth by the QIAT in its assessment. Overall, we find the assessment to be fair. We are particularly satisfied with the relatively good feedback on the proposed legal and governance framework. It is our belief that those aspects are critical, foundational components that need to be carefully constructed to ensure a payment system that meets the task force’s criteria. Without it, there is no way to guarantee inclusion, ubiquity, and competition. Technical interoperability alone does not deliver these virtues when proprietary business interests are unchecked and allowed to create fragmentation in the payment system.

We are also encouraged that the QIAT assessed the proposal very effective on most of the speed related criteria. Most every financial institution has an interface with one or more networks for real-time transaction processing. As the industry builds its faster payments solutions, we believe there is significant value in leveraging these existing interfaces. It will be much easier to add incremental enhancements to these interfaces to support new use cases and contextual data than creating an entirely new infrastructure from scratch. The proposal timeline provides for a phased migration path from ISO 8583 to ISO 20022.

We had hoped that some of the QIAT’s narrative in its executive summary would be adjusted after our Q&A during the preliminary draft assessment. One such passage in the executive summary states, “As is, the solution does not advance the payment system broadly, but rather focuses on making it easier for debit networks to compete with "direct-connect" banks.” This narrative is unfortunate. It was not a stated or implied goal of the proposal. We had communicated to the QIAT that SHAZAM is owned by financial institutions and exists to help them compete in the payment system. The proposal’s requirement that financial institutions interchanging transactions join the sharing arrangement is to avoid situations where financial institutions could be excluded from the payment system. Such exclusion creates fragmentation and a competitive disadvantage for those unable to transact within a de facto network. Only financial institutions can hold depository accounts, sponsor service providers, and warrant transactions in the payment system. The proposal seeks to strengthen fair competition with equal access to the payment system for all financial institutions. It does not position networks or service providers to compete with banks.

The executive summary suggests that the proposal, “seems to be a request for a regulatory requirement that would force networks to share transactions,” and that, “If the requirement to share transactions is delivered, smaller networks such as Shazam could compete more effectively against larger networks, as the value of scale would be diminished.” We wrote back to the QIAT that SHAZAM has sufficient scale to compete effectively. We said that the problem with fragmentation, caused by the lack of sharing, is that participants (financial institutions originating and receiving transactions) may have no choice but to join a network just because of its coverage. They do this not for the network’s feature benefits or more advantageous pricing achieved through scale, but rather for its ubiquity of access. SHAZAM is not advocating for regulatory intervention. We would like to see the industry coalesce around a governance model consistent with the values implied in the task force’s faster payments criteria. Ultimately, financial institutions and public policy makers will need to determine how that is achievable.
SHAZAM PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

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


Seems like a very incomplete solution but would work very well for P2P.

The Usability rating within Ubiquity assessment is unfair. The solution does provide a 24X7X365 process and offers simplicity for routing.

U.4. Contextual data capability should be “not effective,” rather than “somewhat effective.” IF the system perpetuates ISO8583, then there is no improvement to a system in an area that should be easy to enhance. An optimal solution must incorporate ISO 20022. Also, E.4 should be downgraded to “not effective” for a similar reason.

E.1. Efficiency “enables competition” should be “Effective” rather than “somewhat effective”: the solution should reverse the “network effect” that gives larger networks a competitive advantage. Additionally, the system allows processors/networks to charge a transaction fee.

G.1. Effective Governance: should be “not effective” rather than “effective.”

G.2. Inclusive Governance should be “not effective,” rather than “effective.” The proposal would only draw members of its governance body from industry groups. This is wrongheaded. A governance body should include not just providers, but should also draw from different user groups: municipal governments, end-user consumers, small businesses, universities, etc.

Legal Framework: Shazam’s proposal brings up an important concern, specifically the imperative to hold non-banks to the same standards as banks for how they treat consumers. Shazam’s proposal speaks to this need, but it should be the case that any and all systems do so.

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 applies to retail only, and not to commercial. The solution has no written network rules. The solution's legal and governance frameworks are incomplete.

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

U.5 – Cross-Border Functionality should be rated Not Effective due to lack of detail in how transactions can be done through this solution for International transfers.

Interesting proposal and feasible framework utilizing the existing debit networks. Thank you for this submission.

Leverages existing PIN debit network that is very familiar with FIs and customers. Looking to allow individual service providers to determine best alias to use and tie with actual FI account number. Not so much as a new technology solution, but an effort to drive updating rules and regs to open up to be able to expand to support changing market demand and need to sharing of data and oversight. Utilize PIN as golden rule for security—fast clearing and settlement.

While I believe the proposal was fairly assessed, building upon the existing card network infrastructure is something that is now in place and can be built upon in the future. The proposal is not conceptual and there are no leaps of faith necessary in order to make this system work. Can work under the existing rules and governance structure and is something that community institutions can offer their customers.

The focus of this proposal is information sharing, a governance model and some very specific mandates. From that foundation, I would not rate U1 - accessibility as being "effective." It is at best "somewhat effective." For legal and governance frameworks, I disagree with the QIAT arbitrary ratings for L1, L2, L3, L4, G1 and G2. Given that these frameworks are still works-in-process, the ratings should be one level lower.

This solution is consistent with the guidelines and only proposes to use current networks to manage payments. The ability to select which alias they wish to use for a payment is helpful. But it is also looking at prefunding or FedWire for immediate settlement.

The Shazam proposal is consistent with the guidelines set around the effectiveness criteria.

Enables competition should be rated higher, as the proposed solution would connect all bank accounts as well as give access to non-banks. Implementation timeframe should be rated higher, as the proposal takes a realistic view of what it would take to enable inclusive governance and ubiquity (i.e., even the Fed task force is taking 2 years to create its paper). Rules are rated too highly, as they are not yet specifically outlined (in areas where new rules are required).
The proposal focuses primarily on developing a governance model for sharing information among broadly defined networks. We don't believe this is a strong proposal for real-time payments. The proposer's timeline is 2 years to build the governance, and a total of 5 years for the implementation, and not supporting all the use cases until later.


With the exception of some wording issues discussed in the QIAT Assessment Response by the proposer, I see this as an appropriate assessment – and I removed the controversial assessment language in that agreement – assuming that the working could easily be worked to a common conclusion.

Aside from the compelling arguments made in the proposal for "data sharing" through forced interoperability, SHAZAM has offered up nothing new—merely changes to existing rules. How the risk associated with the new rules—more accurately, the consequences—will be managed amounts to a gaping hole in the proposal.

The proposal does not provide much detail on how unbanked consumers would benefit from the system. Also, need more detail on how disputed transactions would be handled beyond citing existing law or network rules, which apply to some but not all payment providers.

(1) Required information sharing (2) leverages existing debit network infrastructure so stakeholders are familiar with (3) individual service providers can determine which payment aliases are used (4) available for all channels and devices (5) fast clearing and approval – 1 second (6) real-time fraud protection on debit side.

Solution really only proposes using existing networks (with their existing advantages and drawbacks) to facilitate payments.

Shazam’s self-assessment was virtually in alignment with McKinsey’s. Consequently, it is difficult to argue with the overall assessment. I do believe that Shazam effectively downplayed their own proposal as a current workable and proven payment solution that meets the very effective criteria of speed for the end-user. Their proposal is largely focused on how the debit rail industry should achieve interoperability with standards that if implemented and followed by key participants would result in meeting the very effective level set out in the criteria in most categories, particularly ubiquity and adoption. As a result it would seem that although the McKinsey’s assessment fairly represented the proposal against the criteria as submitted, the proposal itself appears to have been offered as an industry call for standards and less as an illustration or promotion of Shazam’s practical and functioning payment solution.

Proposal was lacking in several criteria, which was accurately assessed by the QIAT.

I thought the assessment was right on target for this. I had concerns with settlement, governance ubiquity and safety and the QIAT did a good job of calling out those weaknesses.
The assessment properly describes the limitations of the proposal as a solution.

**TASK FORCE SOLUTION-ENRICHING COMMENTS**

**Ubiquity**

This does not address all of the use cases for our member experience. Also how does remittance get processed?

The solution could be enriched to describe the process for mandatory interoperability among debit card networks as noted in the proposed solution. Additionally, the proposal could be expanded to describe how business to business transactions might be handled and how contextual data for both business and consumer transactions might be made available to the payee.

The proposal lacks details necessary to make many determinations. As an end-user, this scheme is not proposing anything new, but changes to existing structures that, it seems, would help their business, but has not proposed a new solution.

Describe further how networks’ sharing of directories occurs in order to reach all downstream accounts. More fully describe how tokens are provisioned and where they are maintained.

Since this is running on the existing card systems, it does not allow for adequate movement of remittance data so it does not adequately address B2B.

U.1 Accessibility – Somewhat Effective, limitations with this solution as it supports only retail payments and a later phase “commercial accounts” will be added, with the hurdle that all networks “must” participate in the network.

U.2 Usability – Not Effective, not clear as to the key “role in relation to the solution’s authentication in relation to the individual networks is likewise unclear.”

U.3 Predictability – Not Effective, relies on existing debit network “rules, requirements and processes” and poses a risk of ensuring how predictable this solution will be.

U.5 Cross-border functionality – Not Effective, “has several networks from which participants may choose to conduct a cross-border transaction” – but not a solid proposal as to how the solution has its own strength to provide cross-border transactions.

U.6 Applicability to Multiple Use Cases – Not Effective, the most common uses cases are not supported at inception, but rather in phases as long as a five-year plan, it would be difficult that faster payment solution could operate within this implementation fragmented timeline.

The proposal does well to emphasize the evolution of debit/EFT networks and to remind the TF that previously perceived limitations may be mitigated or absolved (e.g., with the advent of smartphones, a debit transaction no longer requires a card to intuit a transaction). Unfortunately, as a network-centric
proposal, the submission offers little detail on the auxiliary solutions needed to support this thesis. Greater discussion on the following ideas—even if theoretical—would’ve been well-received: directory, enrollment, error resolution, and interaction by the unbanked.

While SHAZAM-defers third-party sponsorship and means of access to participating FIs, it is notable that the term “API” isn’t mentioned once in the proposal. Hopefully, the system rules would shine greater clarity on the topic of modern access.

SHAZAM uses their experience to pinpoint and share the governance and interoperability challenges presented by a multi-network system. While not 100% comparable, SHAZAM (and other debit/EFT networks) are uniquely positioned to help lead this discussion and offer best practices for a fair and open governance model. It would be interesting to see how the Solution would account for non-debit/EFT-based system.

While it guarantees good funds delivery, SHAZAM’s proposal still operates on existing debit/EFT networks. If existing stakeholders can simplify their business interests, encourage greater access, and pass on more price savings to the end-user (through the noted standardization and governance) SHAZAM proposes a technically feasible and endorsable model.

Fair and open access relies on competition at all levels—from infrastructure to instrument. SHAZAM believes the biggest threat of failed interoperability is the emergence of dominant players (which would inherently act or lean in their own self-interest over time). This is a concern rightfully shared by many in the Task Force. The solution, they believe, is a “universal sharing arrangement” that would serve as “a backbone that level sets messaging, backstops against predatory pricing, and insulates against discriminatory access.” Furthermore, the proposers state, "Networks will still be free to differentiate on the value they provide within their networks, but the value of their inter-network capability would be universal." In an industry without dedicated regulatory oversight to ensure competition (as is the case in many other countries), SHAZAM offers a strong argument for the protection of competition that spans all proposals. To bolster this claim, SHAZAM and other networks should bring in third-party interests in the creation of the network’s agreement and rule-making process (not just governance).

How the unbanked or unenrolled receive a payment token (needed in order to participate and receive funds) is not explicitly discussed, but is inferred. Would be great to see how SHAZAM envisions the adoption and utilization in such a use case.

Doesn’t address all use cases and use cases addressed are phased in.

Customer experience varies from network to network.

Not a clear plan for helping unbanked.

Interesting concept.

**Efficiency**
Meets a critical component of ease of routing by using existing card rails.

We need more information on the "why" and the "how."

The solution could be enriched to describe how the payment process might be enhanced to deliver faster payments within the debit card network.

Discuss more fully how value-added services can be implemented, while sustaining consistency of the fully-integrated networks. With remittance flow, describe where the info is obtained (by whom) and how it is formatted into the URL in a way known to all parties.

E.1 Enables competition – Not Effective, solution relies on existing networks, and is difficult to envision how the regulations, rules and requirements will be brought together among the participating debit networks.

E.3 Implementation timeline – Not Effective, the 5-year timeline seems to leave a huge gap in taking this solution for faster payments, as the first 2 years will be spent on setting up a governance structure, and making difficult to be a real-time faster payment solution.

E.7. Exceptions and investigations process, Not Effective, the responsibilities are shifted to the individual network participants, thereby posing a risk of meeting uniform standards within the solution.

Implementation timeline is pragmatic and reinforces an open and inclusive approach. This should be weighted thoughtfully when comparing the proposed timeline to the arbitrary timeline found in the Criteria requirements.

SHAZAM’s proposal calls for debit networks to absorb the costs of a new, faster system. This may be attractive to everyone on top of the network (minimizes change requirements/costs), but does require all existing networks to join and agree to a handful of processes and standards (i.e., message format, error resolution, alias processing, etc.). How this sits with other networks is not discussed.

Template requirements do not allow proposers to share pricing information; however, the per-transaction cost of a Debit 2.0 network (such as this) needs to be discussed to understand the overall value it brings to the market. (NOTE: the proposal does argue that the new solution would bring great efficiencies to its stakeholders.)

Resiliency concerns.

Financial Institutions do not have to provide payment visibility.

Outdated messaging format.

Debit networks would have to make a lot of changes, may face a lot of resistance.

Safety and Security
How will they address the security issues with a debit pull system?

Appreciate the focus on fraud prevention by giving a monitoring solution out the door.

It is not clear where individual networks would retain their own risk-related rules, or where new overarching rules would be put in place – describe specifically what would be new.

Removing account numbers and PII from the payment flow is an accepted method of protecting this sensitive data, but leaning on PCI for security guidance gives some pause, as the governance of PCI is highly insular. I would like to see a more thorough assessment of the authentication protocols that are supported and required/recommended for S.10. Other proposals specified “two-factor” or “PIN” security, so I am surprised to not see that sort of language in this proposal.

Mandatory information sharing may not be accepted.

Relies on existing debit network policies and procedures, especially for the safety and security criteria.

Data privacy concerns.

Risk management still on the FIs and not shared.

No clear guidelines on fraud sharing information.

S.6 Fraud information sharing – Somewhat Effective, more information is needed as to the adoption of a “centralized or federated” model. Is important to define how the sharing of fraud information will be aligned between the debit networks.

S. 11 Participation requirements, Somewhat Effective, participation agreement will need further enhancements as to the role of the FIs and non-banks and their responsibilities.

Does not seem to really add anything new to existing systems in place.

Speed (Fast)

I do not see how the current proposal will meet the speed deadline.

The solution could be enriched by describing the process to speed up the clearing and settlement of debit network transactions and how the debit card networks might interoperate with other faster payments solutions.

This is an existing solution. It does not meet the criteria of a real-time payments solution.

F.4 Fast settlement among depository institutions & regulated non-bank account providers – Not Effective, relies on existing infrastructure ACH and Fedwire, which are not aligned with real time faster payments.

Does not add any new ideas to systems already in place, which do not meet clearing speed criteria.
Legal

Describe specifics of rules that would need to be agreed to by participants.

L.5 Intellectual property – Somewhat Effective, further clarification is needed among the participating networks as to the IP property rights.

Governance

I think 2 years for the governance is too long. I would like to see more on how then the length.

The Shazam proposal could be enriched if it further described the changes needed within the debit network governance for all parties (including direct-connect banks) to allow for B2B and P2B transactions and transaction sharing, along with contextual data and interoperability.

This proposal asks for change in existing rules and regulations. Once those are in place, it suggests a not for profit organization with rules-making authority. The proposal goes on to say that to meet inclusion standards there will be "equal representation." Without defining what equal representation means it is difficult to know if this is sufficient. From an end-user’s perspective it is important that end-users have a voice and are heard. Does equal mean that each segment has the same number of representatives or is the representation equal to some other expectation or benchmark?

Two years to build governance rules is too long. The proposal seems to focus more on creating the governance than on building a real-time payments solution.

G.1 Effective governance & G.2 Inclusive governance – Somewhat Effective, Effective -“suggests industry formation of a non-for-profit membership organization with rules-making authority for its participants.” However, the proposal does not state how overall decisions will be made.

Inclusive –“rules-making organization will be structured in a manner that provides equal representation and voting rights on important issues as rules, pricing, and specifications.” “It is a fundamental governance assumption that these networks will interchange transactions.” Implementation timeline – “Governance -2 years”"

Very well-constructed governance structure with "equal representation and voting rights on important issues." I believe this is precisely what the FPTF was looking for in the criteria around governance.

5-year phased approach plan to deliver use cases after a governance model is set up seems too long (governed by central operator/association that is independent).
Ubiquity

- *This does not address all of the use cases for our member experience. Also how does remittance get processed.*

The proposal addressed all of the use cases requested by the task force. It is unclear what additional use cases the commenter seeks, but it is likely they are a type already classified. Remittance falls in the B2B or C2B categories, where additional contextual information may be passed with the credit to the company's depository financial institution. The sender service provider may include in the transaction the remittance detail itself or a URL that may be used by the recipient to retrieve the detail. The company's depository financial institution or an affiliated service provider pass the remittance detail to the company.

- *The solution could be enriched to describe the process for mandatory interoperability among debit card networks as noted in the proposed solution. Additionally, the proposal could be expanded to describe how business to business transactions might be handled and how contextual data for both business and consumer transactions might be made available to the payee.*

The proposal calls for the creation of a governance body that would create the rules that require universal sharing. Those network operators and financial institutions that choose to join in the governance body would be bound by its rules. It is possible, perhaps even likely, that some network operators and financial institutions would join only by regulatory or statutory requirement. Those are public policy decisions that are outside the scope of our proposal.

The rules will specify the standards that are used to convey contextual data and the network operators and their participants will need to develop support to pass the information through their systems.

- *The proposal lacks details necessary to make many determinations. As an end user, this scheme is not proposing anything new, but changes to existing structures that, it seems, would help their business, but has not proposed a new solution.*

The proposal aims to provide a governance framework for a faster payments system that provides for competition, inclusion, and ubiquity. While many solutions could operate within that framework, making simple enhancements to an existing infrastructure so it fits the task force criteria seems to be a pragmatic approach than creating an entirely new solution.

- *Describe further how networks' sharing of directories occurs in order to reach all downstream accounts. More fully describe how tokens are provisioned and where they are maintained.*

The governing body will specify the standards for tokens, their provisioning, and how they are used by service providers and senders downstream from the accountholder's depository financial institution. There are existing standards that could be leveraged, such as those being created by EMVCo.

- *Since this is running on the existing card systems, it does not allow for adequate movement of remittance data so it does not adequately address B2B.*

The comment seems to assume that there will be no changes to the status quo. The proposal states that the B2B use cases will be realized after enhancement of the existing messaging to convey contextual data and yet further through migration to ISO 20022.
SHAZAM Responses to Proposal Enriching Task Force Comments

- **U.1 Accessibility** – Somewhat Effective, limitations with this solution as it supports only retail payments and a later phase “commercial accounts” will be added, with the hurdle that all networks “must” participate in the network.

- **U.2 Usability** – Not Effective, not clear as to the key “role in relation to the solution’s authentication in relation to the individual networks is likewise unclear”

- **U.3 Predictability** – Not Effective, relies on existing debit network “rules, requirements and processes” and poses a risk of ensuring how predictable this solution will be.

- **U.5 Cross-border functionality** – Not Effective, “has several networks from which participants may choose to conduct a cross-border transaction” – but not a solid proposal as to how the solution has its own strength to provide cross-border transactions

- **U.6 Applicability to Multiple Use Cases** – Not Effective, the most common uses cases are not supported at inception, but rather in phases as long as a five-year plan, it would be difficult that faster payment solution could operate within this implementation fragmented timeline.

From our experience, technology is easier to change than business arrangements and rules. We believe an undertaking like this would require significant collaboration and negotiation between stakeholders. Other proposals may cite shorter timeframes, but they’re offering proprietary solutions.

Without an incumbent network willing to share for international transactions, the solution would need to create correspondent banking relationships in the other countries and then get financial institutions in those countries to interchange transactions. That is challenge that any solution faces.

**Cross border payments**

- **How the unbanked or unenrolled receive a payment token (needed in order to participate and receive funds) is not explicitly discussed, but is inferred. Would be great to see how SHAZAM envisions the adoption and utilization in such a use case.**

Service providers will be sponsored into networks by depository financial institutions, allowing them to provide payment services to unbanked individuals. To the network, the accounts, the tokens, and the payments will be similar to those owned by banked account holders.

- **Doesn’t address all use cases and use cases addressed are phased in customer experience varies from network to network not a clear plan for helping unbanked**

There will likely be some provisions that the governing body will require all member networks to include in their own rules to provide a consistent experience across networks.

**Efficiency**

- **Discuss more fully how value-added services can be implemented, while sustaining consistency of the fully-integrated networks. With remittance flow, describe where the info is obtained (by whom) and how it is formatted into the URL in a way known to all parties.**

To become members in the sharing organization, networks will need to agree to add certain provisions to their rules. Some of those provisions would provide for a framework for service providers to deliver value-added services in a manner that is consistent across networks.

The proposal suggested the use of ISO 20022 remittance advice for the remittance information passed with the transaction. If a URL is provided instead, the information retrieved would be formatted using the same standard.
SHAZAM Responses to Proposal Enriching Task Force Comments

• **E.1 Enables competition – Not Effective**, solution relies on existing networks, and is difficult to see envision how the regulations, rules and requirements will be brought together among the participating debit networks.

  E.3 Implementation timeline – Not Effective, the 5-year timeline seems to leave a huge gap in taking this solution for faster payments, as the first 2 years will be spend on setting up a governance structure, and making difficult to be a real time faster payment solution.

  E.7. Exceptions and investigations process, Not Effective, the responsibilities are shifted to the individual network participants, thereby posing a risk of meeting uniform standards within the solution.

The commenter’s remarks regarding E.1 and E.3 are redundant with other commenters’ remarks and are addressed by us elsewhere in this document. Regarding E.7, the proposal indicates that network rules will provide for standards for disputes and exception item processing. Those standards will be promulgated through participating networks down to participating financial institutions and their sponsored service providers. This is consistent with existing practice through the payments system.

• **Implementation timeline is pragmatic and reinforces an open and inclusive approach. This should be weighted thoughtfully when comparing the proposed timeline to the arbitrary timeline found in the Criteria requirements.**

  SHAZAM’s proposal calls for debit-networks to absorb the costs of a new, faster system. This may be attractive to everyone on top of the network (minimizes change requirements/costs), but does require all existing networks to join and agree to a handful of processes and standards (i.e. message format, error resolution, alias processing, etc.). How this sits with other networks is not discussed.

  Template requirements do not allow proposers to share pricing information; however, the per transaction cost of a Debit 2.0 network (such as this) needs to be discussed to understand the overall value it brings to the market. (NOTE: the proposal does argue that the new solution would bring great efficiencies to its stakeholders).

  Resiliency concerns; Financial Institutions do not have to provide payment visibility; outdated messaging format debit networks would have to make a lot of changes, may face a lot of resistance.

  We appreciate the commenter’s line of inquiry about efficiency. We believe it will be more efficient to add volume to an existing infrastructure than to create an entirely new infrastructure with new overhead offset by relatively low volume in comparison. We also contend in the proposal that a benefit to this governance model is that it ensures competition amongst network operators to encourage a drive to efficiency.

**Safety & Security; Category**

• **HOW WILL THEY ADDRESS THE SECURITY ISSUES WITH A DEBIT PULL SYSTEM?**

  It is not clear where individual networks would retain their own risk-related rules, or where new over-arching rules would be put in place – describe specifically what would be new.

  S.6 Fraud information sharing – Somewhat Effective, more information is needed as to the adoption of a “centralized or federated” model. Is important to define how the sharing of fraud information will be aligned between the debit networks.

  S. 11 Participation requirements, Somewhat Effective, participation agreement will need further enhancements as to the role of the FIs and non-bank and their responsibilities.

  Removing account numbers and PII from the payment flow is an accepted method of protecting this sensitive data, but leaning on PCI for security guidance gives some pause, as the
SHAZAM Responses to Proposal Enriching Task Force Comments

governance of PCI is highly insular. I would like to see a more thorough assessment of the authentication protocols that are supported and required/recommended for S.10. Other proposals specified "two factor" or "PIN" security, so I am surprised to not see that sort of language in this proposal.

- mandatory information sharing may not be accepted relies on existing debit network policies and procedures, especially for the safety and security criteria data privacy concerns risk management still on the FIs and not shared no clear guidelines on fraud sharing information

- S.6 Fraud information sharing – Somewhat Effective, more information is needed as to the adoption of a “centralized or federated” model. Is important to define how the sharing of fraud information will be aligned between the debit networks.

S. 11 Participation requirements, Somewhat Effective, participation agreement will need further enhancements as to the role of the FIs and non-bank and their responsibilities.

Authentication types to pass between a transaction originator and the accountholder’s depository financial institution will need to be standardized across the sharing arrangement to ensure there is consistency in user experience and risk management. These specific rules could not be described further at the time of proposal, because they will be a derivative work of the not-for-profit governing body.

Speed (Fast)

- I do not see how the current proposal will meet the speed deadline.

The timeline could be accelerated if the participants can drive the process faster. We cited what we thought were conservative timeframes.

- The solution could be enriched by describing the process to speed up the clearing and settlement of debit network transactions and how the debit card networks might interoperate with other faster payments solutions.

We agree this would be good ground to explore further.

- This is an existing solution. It does not meet the criteria of a real-time payments solution.

It is true that the proposal largely leverages existing infrastructure and capabilities. We believe that is a positive attribute. It is opinion that it does not meet the criteria. The assessments indicate it meets several aspects of the criteria.

- F.4 Fast settlement among depository institutions & regulated non-bank account providers – Not Effective, relies on existing infrastructure ACH and Fedwire, which are not aligned with real time faster payments

Without correspondent accounts held at the network’s’ bank, the network needs a means to perform settlement. Perhaps the solution could be improved by requiring participating financial institutions to hold correspondent accounts. We thought it was more pragmatic to use their existing accounts at the Federal Reserve for settlement.

- does not add any new ideas to systems already in place, which do not meet clearing speed criteria

The commenter may be confusing clearing with settlement. The solution absolutely provides for fast clearing, which is done technically at the same time as authorization, within sub-second time on average.
SHAZAM Responses to Proposal Enriching Task Force Comments

Legal

- Describe specifics of rules that would need to be agreed to by participants.
  The rules could not be described further at this time, because they will be a derivative work of the not-for-profit governing body.

- L.5 Intellectual property – Somewhat Effective, further clarification is needed among the participating networks as to the IP property rights.
  The stakeholders that gather to create the bylaws will determine what IP provisions are included.

Governance

- I think 2 years for the governance is too long. I would like to see more on how then the length.
  The timeline could be accelerated if the participants can drive the process faster. We were just citing what we thought were conservative timeframes.

- The Shazam proposal could be enriched if it further described the changes needed within the debit network governance for all parties (including direct-connect banks) to allow for B2B and P2B transactions and transaction sharing, along with contextual data and interoperability.
  We agree this would be good ground to explore further.

- This proposal asks for change in existing rules and regulations. Once those are in place, it suggests a not for profit organization with rules-making authority. The proposal goes on to say that to meet inclusion standards there will be "equal representation". Without defining what equal representation means it is difficult to know if this is sufficient. From an end users perspective it is important that end users have a voice and are heard. Does equal mean that each segment has the same number of representatives or is the representation equal to some other expectation or benchmark?
  We did not believe it prudent to advocate for a particular voting structure, because creating an organization like this will require iteration of negotiation amongst stakeholders to define classes of membership and the weighting in representation they will have in voting.

- Two years to build governance rules is too long. The proposal seems to focus more on creating the governance than on building a real time payments solution.
  The timeline could be accelerated if the participants can drive the process faster. We cited what we thought were conservative timeframes.

- G.1 Effective governance & G.2 Inclusive governance – Somewhat Effective, Effective - “suggests industry formation of a non-for-profit membership organization with rules-making authority for its participants.” However, the proposal does not state how overall decisions will be made.
  Inclusive –“rules-making organization will be structured in a manner that provides equal representation and voting rights on important issues as rules, pricing, and specifications. “It is a
fundamental governance assumption that these networks will interchange transactions”
Implementation timeline – “Governance -2 years”

This would need to be defined in the bylaws for the not-for-profit governance body that would be created. There will be negotiation amongst stakeholders that create the bylaws to define the mechanics of decision-making, including classes of membership and the weighting in representation they will have in voting.

• 5 year phased approach plan to deliver use cases after a governance model is set up seems too long (governed by central operator/association that is independent)

The timeline could be accelerated if the participants can drive the process faster. We cited what we thought were conservative timeframes.
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: SHAZAM, Inc.

Summary Description of Solution:

The solution is less a technical proposal than it is a case for the universal sharing of information and equitable participation among the existing debit networks. It seeks a broader definition of “network”: in Shazam’s view, not only debit networks should be considered to be “networks”; any two or more financial institutions (FIs) that directly exchange transactions should also be redefined as “networks.” These FI networks, then, should be required to share information with other networks just as ACH operators are required by NACHA to share transactions.

The proposal focuses primarily on developing a governance model for sharing information among these broadly defined networks. “Sharing information” is defined as one “payment brand [i.e., network] facilitating a transaction into another payment brand” (p. 6). Shazam maintains that requiring information-sharing would address the “payment brand participation gap” and achieve functional interoperability among debit networks.

Based on this premise, the solution facilitates debits and credits to a deposit account in real time using a real or tokenized account identifier. The solution relies on existing network rules, processes, and procedures related to clearing and settlement. The solution addresses the network aspect only, and responsibility for end-user requirements related to authentication, access channels, disputes, etc. will belong to the connecting providers.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths

– The solution proposes a governance framework for competing networks based on the requirement to “share information” that the proposer believes will facilitate sharing and thus interoperability among debit networks.

– By leveraging existing debit network infrastructure, processes, and capabilities, the solution allows for ubiquitous end-user access, either through a participating FI or through a regulated, non-financial institution holding a master account at a participating FI. The proposal does not depend on any new directory capabilities but suggests that payment account token prefixes continue to be used to route transactions, that networks continue to exchange directories, and that new concepts be introduced to extend existing directories.

– Individual service providers can determine which alias(es) (e.g., cell phone number, email address) they wish to support for payment and can connect the alias information to the payment account token.

■ Areas for improvement and enhancement

– The solution calls for mandatory interoperability among debit card networks. The existing card networks will provide most specifications, and a future governance body such as NACHA, the Federal Reserve Bank, or a new, not-for-profit rules-making organization would develop and maintain sharing rules. The solution calls for the use of a system that is readily available today, and that does not modify the payment process or experience to deliver faster payments or new
use cases. Accordingly, the solution merely increases the reach of current solutions built on a single network.

- The solution relies on existing debit network policies and procedures to support all stages of the transaction, including clearing and settlement. Each network would continue to operate as it does today, but would support the routing and transmission of additional, “out of network” transactions. The solution also depends on a token to drive the alias, but it does not describe how tokens other than card numbers would be created, nor does it describe where this information would be made available to network participants.

- The solution leverages existing settlement solutions and calls for the use of prefunding or Fedwire for settlement of urgent payments. The solution makes no mention of connecting to TCH (The Clearing House) or any other real-time networks once available in the market. Essentially, this proposal is a request for networks to share transactions.

- The solution has a five-year implementation timeline with a general framework for building its rules, but the proposal lacks specifics.

■ Use cases addressed

- The solution is not applicable to all use cases. Major elements are missing (e.g., remittance-sharing) for specific use cases, such as B2B. If all described upgrades are executed, the solution’s technical design will support all use cases over time.

- As proposed, Phase I of the solution will last for two years and focus on the creation of governance rules. Phase II spans one year and calls for the delivery of “basic functionality”: P2P (person to person) and B2P (business to person) use cases. Phase III spans one year and calls for the introduction of B2B (business to business) and P2B (person to business) capabilities. The delay in delivering any use case in the first two years is due to the need first to design a governance plan and then to determine how to support interoperability.

■ Proposer’s overall ability to deliver proposed solution

- This proposal is high-level and requires a substantial change in the debit networks’ operating models in order to be successful. To effect the change the proposer seeks, the definition of “network” must be fundamentally modified to include direct-connect banks, and networks will have to implement the ability to share transaction information to support ubiquitous access. This level of ubiquity for information-sharing is likely to be achieved only via mandate.
ASSESSMENT

Ubiquity

U.1 Accessibility

Very Effective    Effective    Somewhat Effective    Not Effective

Rationale:

The proposal’s objective is to eliminate “fragmentation [of] and discriminatory access” to the payment system. To accomplish this goal, all networks must participate in the system. The proposer does support the notion that a valid business case may exist for certain direct-connection relationships to remain intact.

As proposed, the solution and its accessibility rely entirely on the mandated sharing of transactions and full adherence to existing debit network rules. To enable interoperability (U.1.6) among participating networks, a new rules-making organization will need to be created to develop a common set of rules. The proposal sets forth a high-level, five-year implementation plan to create its industry-level governance model (U.1.5); the first two years of the plan are focused on aligning participating networks through the creation of solution governance.

The solution facilitates payments to and from accounts that can be linked to a debit network (U.1.1). At launch, the solution considers only retail accounts, with commercial accounts to be added in a later phase. Any regulated, non-bank PSP (payment services provider) can have access to the solution as long as it holds a master account at a participating FI (U.1.1), thereby providing access to the unbanked (U.1.4).

However, the solution does not initially support payments to and from all end-user accounts (U.1.2). The proposer can strengthen the proposal by detailing a clear plan to accelerate specific, unmet use cases such as P2P and B2P. For example, in the current proposal, those use cases will be supported in Year 3 of the implementation plan, while B2B and P2B are part of Phase III deployment in Year 5. Accelerating the inclusion of those use cases could enhance the proposal’s viability. It could be further improved by providing a clear plan showing how international cross-border payments will be enabled through a collection of domestic debit networks, as these networks only operate in USD.

U.2 Usability

Very Effective    Effective    Somewhat Effective    Not Effective

Rationale:

The solution is available to users 24x7x365 through a variety of devices and channels (U.2.1, U.2.3). For authentication, the solution supports the use of tokenized account information (U.2.2), but it is not clear which alias options (e.g., email address, cell phone number, etc.) will be supported across participating networks to ensure consistency. The solution’s authentication role in relation to the individual networks is likewise unclear, although the proposal does state that service providers are responsible for authentication (p. 10).
While the solution is device- and channel agnostic (U.2.1), and the transactions set for universal sharing should include all transaction types, the governance body needs to define which transaction types are mandatory for the solution.

Much of the end-user’s experience is the provider’s responsibility and will be subject to existing debit network requirements and, potentially, inter-network requirements. As a result, the customer experience could vary from network to network (U.2.3). The proposal could be enhanced by explaining how some of this potential variability could be avoided by establishing a set of minimum standards in the network participation and operating rules. Additionally, payment system rules regarding notifications need to be developed to require and enable payment status notifications to payees (U.2.4).

U.3 Predictability

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

**Rationale:**

The solution relies heavily on existing debit network rules, requirements, and processes, and it is unclear whether these requirements and processes can be aligned across networks to ensure predictability. The solution is channel- and device-agnostic, as service providers determine which devices and channels are acceptable, with limited constraint by network rules or applicable regulations. Essentially, this flexibility facilitates competition by allowing service providers to differentiate end-users’ experience.

To facilitate a consistent experience for end-users’ interactions with each other and other parties (U.3.3), the solution leverages ISO 8583, a legacy messaging format common among debit and ATM networks that is not used broadly beyond POS and ATM transactions. The proposal contemplates the use of translation engines for various “dialects” (each network’s particular implementation of ISO 8583) (p. 11). The proposal could be strengthened by detailing a plan to support the emerging ISO 20022 messaging standard rather than taking a “wait-and-see” approach (p. 11).

U.4 Contextual data capability

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

**Rationale**

The solution’s standard messaging format is ISO 8583, a legacy format that, in its current iteration, does not support the transmission of contextual data. Without the use of ISO 20022 or an expanded translation capability, the solution cannot provide detailed remittance data. The proposal does discuss adding support for contextual data, but the capability will not be introduced until Phase 3, in conjunction with commercial use cases B2B and P2P.

The solution could be enhanced by introducing contextual data capability into an earlier phase, likely Phase 2, given the current implementation timeline. (Phase 1 is the two-year governance phase, while Phase 2 is a one-year effort to build basic interoperability.) The proposal suggests that payees could access remittance data through a URL (p. 14) or QR code (p. 16) associated with the transaction; the proposal could be strengthened by providing details about the specific information.
that will be provided in the URL or QR code and describing how the URL or QR code will be transmitted i.e., via ISO 8583 or another communication channel).

**U.5 Cross-border functionality**

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

**Rationale:**
The proposal could be strengthened by clarifying how the solution would enable convenient, cost-effective, timely, secure, and legal payments from other countries (U.5.1). The proposal indicates that some of the participating debit networks would support international transactions, but it needs to explain how the solution itself will support those transactions (U.5.2). The proposal would be further enhanced by discussing which networks will participate, which networks have cross-border functionality, and how cross-border functionality can be extended to end-users of other debit networks. The inclusion of cross-border transactions is currently slated for Phase 2; the proposal could be improved by detailing how this capability will be added (U.5.5).

**U.6 Applicability to multiple use cases**

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

**Rationale:**
According to Shazam’s five-year implementation plan, the solution will support the main use cases, but not immediately. The first two years (Phase 1) will be spent designing a governance plan; the following year (Phase 2) will be spent building basic interoperability. This second phase will support the P2P and B2P use cases. In Phase 3, the “commercial enablement” phase, the solution will enable B2B and P2B payments and will add ISO 20022 capability to support remittance information. As mentioned above, the solution could benefit from accelerating the phases of its implementation plan.

**Efficiency**

**E.1 Enables competition**

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

**Rationale:**
The solution would create a single large network consisting of multiple debit network providers; it thus could potentially increase the number of networks a participating FI could leverage (E.1.2) and would benefit smaller networks that have less reach and functionality than their larger counterparts. In theory, an FI could have a relationship with any debit network provider and have access to all of the features and functionality of the largest network (E.1.4). FIs will likely be able to choose the lowest-cost provider and to switch between providers without losing core functionality (E.1.1-2). Responsibility for cost disclosures is left to participating FIs (E.1.3).
As discussed in previous criteria, however, the solution relies on existing debit network requirements, rules, and regulations. The proposal could be enhanced by explaining how requirements, rules, and regulations will be aligned across the participating networks (E.1.3 and E.1.4).

E.2 Capability to enable value-added services

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

**Rationale:**

Providers can develop value-added services, but such services fall outside the solution’s immediate scope. Individual networks will develop new products and services beyond the solution’s core functionality to differentiate themselves enough to win direct connection, just as they do today. While this approach could facilitate differentiated functionality and end-user experiences, the ability to introduce new functionality may be limited, given that ISO 20022 will not be available until Phase 3 of the solution. Successful implementation of the solution will allow service providers to choose among a greater number of networks that can provide universal access.

The proposal can be enhanced by explaining how providers can integrate with the solution via open and accessible standards to offer value-added services (E.2.1), as well as how all providers can offer value-added services as long as they adhere to a minimum set of participation requirements (E.2.2).

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:**

As mentioned, the proposal describes a five-year timeline divided into three phases. The first two years of implementation are focused on designing governance rather than on introducing new capabilities into the market. The proposal could be enhanced by indicating which entity will lead this exercise and maintain the documentation once created.

Phase 2 will leverage existing debit network capabilities to deliver basic functionality (B2P and P2P) within 12 months. Commercial transactions (B2B, P2B) will be delivered in Phase 3 (Years 4 and 5).

The solution’s value proposition could be enhanced by accelerating the enablement of use cases (B2B and P2B, for example) and the capabilities required (e.g., contextual data) to support those use cases.
E.4  Payment format standards

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution uses the ISO 8583 format to start, with the use of a translation engine to address dialects (individual networks’ particular implementations of ISO 8583) across networks and to serve as a bridge to the possible adoption of ISO 20022 in the future. Given that ISO 20022 is evolving into a de facto standard capable of supporting expanded contextual data, the proposal would benefit from developing a plan to implement ISO 20022 rather than postponing this implementation until “business needs dictate” it (p. 11) (E.4.4).

ISO 20022 support is necessary to enable international interoperability and to support the inclusion of contextual data in relevant B2B use cases (E.4.1); a more definitive plan to support ISO 20022 would thus be helpful. ISO 8583, however, is interoperable for cross-border transactions among card networks with cross-border capability (E.4.2). Since debit networks already use ISO 8583, message format implementation costs will not come into play until (if) ISO 20022 is implemented (E.4.3). The ISO 8583 message format will be updated through the ISO system (E.4.4).

E.5  Comprehensiveness

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution focuses on providing network capabilities. In concert with FIs, which are responsible for the other aspects of the end-to-end payment process, it 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). To execute the payment process, the solution relies on the debit networks’ existing capabilities and their requirements of participating FIs for initiation, authorization and authentication, clearing, and receipt of transactions.

E.6  Scalability and adaptability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution’s technical design does not support all use cases at the outset, but the B2B and P2B use cases will be supported in the future (Phase 3) (E.6.1).

The solution leverages existing debit networks’ infrastructure, policies, and procedures. While the proposal does not explicitly describe how the individual networks will scale and adapt to support increased volume and new transaction types, it does suggest that latent capacity in the networks can handle any potential network scale issues (E.6.2). The proposal could be strengthened by providing transaction volume forecasts and likely processing or throughput rates (E.6.2). The proposal describes how the debit networks will adapt to ongoing developments (e.g., technological, economic developments) (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 proposal relies on individual network capabilities, rules, policies, and procedures to manage exceptions and disputes.

The proposal can be strengthened by describing how these individual network capabilities will be aligned to provide a consistent end-user experience across the solution’s core functionality and the transactions enabled by the solution. It would beneficial as well if the proposal addressed the aggregation of data or monitoring of transactions for suspicious patterns at the centralized level (E.7.3). The assumption is that the participating debit networks would monitor transactions at a network level, as they do today.

Once written, the solution will have a universal sharing agreement that is expected to include rules to which networks must adhere to participate. It is expected that these rules will normalize the end-user experience to an extent. The proposal suggests that a federated consortium model or a centralized model might be applied to exceptions-handling and investigations (p. 21), but no guidelines or requirements are provided. The proposal could be enhanced by addressing the need for a set of minimum core standards that all member networks must adhere to for handling exceptions in the solution’s operating and participation rules.

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:**

Shazam proposes creating a risk committee to develop an inter-network risk management framework that would leverage individual debit networks’ existing compliance and risk management functions. The risk management committee would serve as part of the solution’s overall governance. As such, it would monitor systemic risk issues associated with the sharing of transaction information, including counter-party risk, business continuity standards, and inter-network fraud reporting. The proposal does not describe how the individual networks’ requirements, standards, and processes would be aligned, defined, and enforced across networks to deliver a consistent risk management approach and end-user experience.

The solution places responsibility for much of the necessary risk management onto participating FIs. The risk management committee will address risks related to settlement (S.1.2); operations (S.1.3); and unauthorized, fraudulent, or erroneous payments (S.1.4); however, the risk management committee is not yet in place (S.1.1). The proposal could be enhanced by discussing how operators and providers will manage the risk they may pose to other participants (S.1.5) and
how the risk management committee will review and update the risk management framework (S.1.6).

S.2 Payer authorization

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

**Rationale:**
The solution leverages the authentication and good-funds authorization practices currently required by participating debit networks. The onus for payer authorization is placed directly on participating FIs, as per network participation requirements. The solution can handle pre-authorized transactions in both single and recurring payment scenarios. The shared network rules and message specifications are in place to ensure a consistent minimum standard across networks for these payments (S.2.2-3).

S.3 Payment finality

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

**Rationale:**
The solution leverages debit networks’ existing capabilities, functionality, and requirements for payments finality, and debit networks require that all payments be authorized to ensure good funds (S.3.1). The shared network rules, while not yet written, should provide a unifying standard for revocability of shared network transactions. The proposal indicates that the rules committee could leverage existing network rules addressing liability, error resolution, adjustments and disputes to create a consensus-driven, normalized set of rules for participants in the universal sharing arrangement (S.3.2-3).

S.4 Settlement approach

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

**Rationale:**
The solution will leverage existing settlement processes and the risk management activities required by participating debit networks (S.4.1). Payments will be settled in central bank funds (S.4.3). To settle transactions in the use cases that will be implemented in Phase 2 (B2P and P2P), the solution will use ACH or wire transfers. For the commercial payment use cases that will be supported in Phase 3 (B2B and P2B), the solution will evolve to accommodate real-time settlement. Phase 3 of the implementation timeline suggests that networks will be able to override default daily settlement and to execute real-time settlement instead. The proposal could be enhanced by clearly describing how real-time settlement will be implemented.

The proposal could be further strengthened by adding rules for managing credit and liquidity risks across the solution and relying less on existing network practices (S.4.2). The proposal states that the solution’s risk management committee will “define safety and soundness policies ensuring
[that] networks participating in the inter-network sharing are protected from counter-party risks” (p. 31).

S.5 Handling disputed payments

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

**Rationale:**

The solution will leverage existing debit network rules, policies, and procedures for handling payment disputes (S.5.1). The solution does not require specific controls applicable to business and government payers, but it does allow for configurable controls, such as transaction limits, alerts, and a fraud monitoring system. Additionally, the solution’s governing organization will appoint a grievance committee responsible for establishing a set of minimum real-time-payment dispute standards for solution participants.

The proposal could be improved by describing how debit network participants already comply with consumer protection laws (S.5.2, S.5.5) and by listing the mechanisms in place to address disputes (S.5.3). The proposal could further be enhanced by anticipating how dispute processes will have to evolve as commercial payment use cases (B2B, P2B) are implemented (S.5.4).

S.6 Fraud information-sharing

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

**Rationale:**

The proposal considers adopting a centralized or federated approach to sharing fraud information (p. 21) (S.6.1). The proposed rules-making association will define this approach. While still conceptual, the proposal suggests that a distributed ledger system may be suitable for the federated model, wherein networks would manage nodes and contribute transactional data. The organization governing the sharing agreement will need to manage or to contract management of a facility for the centralized model. In either model, access to data will be universal and undifferentiated. The solution does support real-time fraud monitoring, but the monitoring will be executed by individual FIs. This real-time monitoring is expected to add less than 100 milliseconds to the authorizing process.

The proposal could be enhanced by establishing a set of decisions that would provide clear guidelines for adopting either the centralized or federated model for sharing fraud information (S.6.1). It can be further strengthened by creating operating rules that provide differential access to data based on roles and responsibilities (S.6.5). Providing functionality to aggregate fraud information to identify patterns could likewise bolster the solution (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 solution includes the creation of a new risk governance structure that would harmonize participating networks’ security controls and policies and then define and set standards for inter-network sharing (S.7.3). The framework that has been described, while not yet up and running, clearly sets forth minimum security standards, including governing security policies, protection of sensitive data, systems configurations, application development, vulnerability, change management, user access, system identification and authentication, physical security, and security testing and auditing.

S.8 Resiliency

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

**Rationale:**

The solution will leverage participating networks’ existing business continuity plans (BCPs) (S.8.2), which are regularly updated and tested (S.8.5). As with the solution’s security standards, the risk management committee will need to adopt a set of minimum real-time-payment resiliency standards. The proposal could be enhanced by detailing how the current BCPs work and defining a standard approach to resiliency across the solution. It can be further improved by addressing the impact that volume increases or the addition of new transactions or services (e.g., contextual data) might have on existing BCPs.

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 debit networks participating in the solution will use payment account tokens and will not require account information or PII (personally identifiable information) to be transmitted along with transactions (S.9.3). All service providers, processors, and networks must comply with GLBA (Gramm-Leach-Bliley Act) and PCI (Payment Card Industry) requirements (S.9.1). Individual participants will manage proprietary directories to support the use of alias information (e.g., email address, cell phone number) (S.9.2). Additionally, any forthcoming guidance from either the Faster Payments or Secure Payments Task Forces will be leveraged when building additional rules for end-user data protection.

The proposal could be strengthened by clarifying how the use of aliases and access to PII stored in directories will align across networks (S.9.1 and S.9.3). It would be helpful for the proposer to explain the networks’ and participating FIs’ roles and responsibilities regarding data protection.
S.10  End-user/provider authentication

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

Rationale:

The solution will leverage existing debit network rules for authentication (S.10.1); these rules align with regulatory guidance and industry standards for end-user authentication (S.10.3). Operating rules will require that certain types of authentication be used in conjunction with some transaction types and may otherwise adjudicate liability based upon the type of authentication attempted and used. Service providers and FIs have the flexibility to adopt authentication methods that suit their use cases and risk tolerance.

The proposal could be strengthened by addressing how the network will ensure that payments reach the intended payee or account (S.10.2), whether strong authentication controls would be applied across all channels (S.10.3), and how authentication models may be changed in response to an evolving threat landscape (S.10.6).

S.11  Participation requirements

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

Rationale:

The solution leverages existing debit network participation requirements but also defines how the association will establish predefined criteria to evaluate participant soundness (e.g., risk-weighted capital, broker deposit ratio, etc.). Member networks will be required to implement procedures to evaluate FI applicants against the developed criteria.

The proposal could be enhanced by detailing how the solution will ensure that participating FIs and non-banks have the operational, financial, and legal capacity to fulfill their obligations (S.11.2).

Speed (Fast)

F.1  Fast approval

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

Rationale:

The majority of Shazam’s transactions are executed end-to-end (E2E) in 400 milliseconds, and transaction approvals take milliseconds. Clearing and approval occur simultaneously. Assuming that participating FIs will comply with existing network speed requirements for providing transaction approval, the solution needs less than one second to route the transaction.
F.2 Fast clearing

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

**Rationale:**

The solution enables fast clearing, as the majority of Shazam’s transactions are executed E2E in 400 milliseconds, and transaction approval takes milliseconds. The solution’s single message format allows posting to occur simultaneously with authorization.

F.3 Fast availability of good funds to payee

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

**Rationale:**

According to the proposal, debit network rules require full funds availability upon receipt of approval. The solution’s baseline features facilitate real-time delivery of guaranteed good funds from payer to recipient. The recipient’s FI can decide to make funds fully available to the recipient at that point, even though settlement does not occur in real time.

The proposal suggests that operating rules will require large commercial funds transfers to use real-time settlement for fast funds availability. The proposal could be augmented by defining the amount that constitutes a “large” commercial transfer.

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

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

**Rationale:**

The solution leverages settlement capabilities that are already in the market (Fedwire, ACH). In Phase 3, originators will be able to request real-time settlement on a transaction, although real-time settlement will not be required.

The proposal could be strengthened by explaining how credit or liquidity risks arising from settlement lags will be addressed (F.4.1). Further, it would be beneficial to address special considerations for settlement among providers in different time zones (F.4.2). The proposer should also consider describing how the introduction of same-day ACH settlement will affect the availability of good funds and inter-network risk management.

F.5 Prompt visibility of payment status

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

**Rationale:**

Participating debit networks will support prompt visibility of payment status. It is up to FIs to decide whether to provide notification to end-users.
Legal

L.1 Legal framework

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

Rationale:
The proposal calls for the use of existing network rules and compliance functions but does not provide any details of existing requirements. The proposal does not identify any new requirements that may be required to deliver alignment across participating networks, or to support real-time settlement in Phase 3. The proposal can be enhanced by clearly describing how the rules will be aligned across all participating networks, and how minimum requirements will be determined. It is suggested that a legal framework will be developed for the inter-network solution.

The proposal acknowledges a need for a legal framework and sets out a fairly detailed plan to complete it, 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 “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:
The proposal states that existing network rules from incumbent networks address the issues delineated in L.2.1 and details the rules for end-users, providers, payers, and payees across a broad spectrum of payments functionality. The proposal could be enhanced by describing how minimum requirements for payment system rules will fill any gaps in existing network rules and ensure alignment across networks.

L.3 Consumer protections

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

Rationale:
The solution leverages existing payment network requirements to support consumers. The proposal could be made more robust by addressing inter-network error resolution rules and procedures (L.3.2). It could be further enhanced by discussing whether end-users, providers, or the payment system may establish consumer protections for payments that augment current consumer protection laws (L.3.3). Further clarifying how requirements will be aligned across network participants to ensure a consistent consumer experience would likewise benefit the overall proposal.
L.4 Data privacy

Very Effective        Effective        Somewhat Effective       Not Effective

Rationale:
The proposal does not directly address data privacy. The solution proposes to leverage and align existing network requirements related to data privacy, but no details of these requirements are provided in the proposal. The proposal can be strengthened by describing how requirements will be applied consistently across participating networks.

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

L.5 Intellectual property

Very Effective        Effective        Somewhat Effective       Not Effective

Rationale:
Members must agree that contributions to the association are the property of the association. In the participation rules, members agree that any contributions they make after joining the association will be the property of the association unless they are declared to be restricted, intellectual property (L.5.1).

The proposal can be strengthened by discussing any due diligence reviews that have been undertaken or will be undertaken to assess potentially applicable intellectual property rights (L.5.1).

Governance

G.1 Effective governance

Very Effective        Effective        Somewhat Effective       Not Effective

Rationale:
The proposal suggests creating a new, not-for-profit membership organization with rule-making authority to provide governance for the solution. Representatives would be selected from industry stakeholder organizations. The development of the governance model will take place in Phase 1 of the solution and is expected to take up to two years. High-level elements of the model have been identified (e.g., publicly available bylaws, the ability of members to appeal decisions, the formation of an appeals or grievance committee, plans to hire an independent auditor, etc.)

The proposal could be improved by describing how decisions and rule-making would take place (G.1.1), how appeals and escalations would be handled (G.1.3), and how independent validation of compliance would be assured.
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:**
Diverse stakeholders/participants will have input and voting rights on important issues such as rules, pricing, and specifications (G.2.2). Board seats will be reserved for public-sector representatives as part of the governance model (G.2.1). All stakeholder classes will be equally represented in committees and working groups (G.2.2-3). The proposer notes that the bylaws should ensure that board rotations allow categories of stakeholders equal opportunity for representation in committees. The bylaws will further require recusal from a committee when a decision directly affects that member (G.2.5).