Faster Payments QIAT

Proposer: InterComputer Corporation

February 21, 2017

TABLE OF CONTENTS

Original Proposal 2

Q&A Response 75

Additional Questions Submitted and QIAT Response 101

Draft QIAT Assessment 117
    (Includes proposer comment in Appendix A & B) 132

Task Force comments 138

Proposer response to Task Force comments 146

Final QIAT Assessment 170
“The proposer, InterComputer Corporation, has declined to grant a license under section 5(b)(iv)(1) of the Faster Payments Task Force Participation Agreement for any Essential Claim incorporated in its Proposal and included in the Final Report. An Essential Claim is any patent or patent application owned by a proposer or an Affiliate of the proposer in any jurisdiction in the world that would necessarily be infringed by implementation of the proposer’s Proposal.

Specifically, InterComputer Corporation has declined to grant a license for any Essential Claim under U.S. Patent No. 8,380,622 entitled “Secure Electronic Payments with Reconcilable Finality”. InterComputer Corporation identified the disclosures in Executive Summary, Pages 5-8 and Part A, pages 13-30, as portions of the Proposal that are relevant to its Essential Claim.

As with all proposals, any entity or person wishing to utilize a proposal should contact the proposer. Neither the Federal Reserve Banks, the Federal Reserve Board, nor the Faster Payments Task Force make any representations regarding the ownership of or the availability for use of any intellectual property disclosed in a proposal, and any entity or person seeking to use part or all of any proposal should secure the appropriate licenses.
Faster Payments Task Force Proposal

The InterComputer Network (ICN)

- InterComputer Interoperating System (IC IOS)
- PrivateLine Payments (PL Pay)
- Trusted Settlement System (TSS)

April 30, 2016
Submitted by: Scott M. Volmar, InterComputer Corporation
Contents

EXECUTIVE SUMMARY ............................................................................................................. 5
USE CASE COVERAGE ............................................................................................................... 9
   Supported Use Case Coverage Summary ............................................................................. 9
   Cross-border Use Case Coverage ......................................................................................... 10
PROPOSAL ASSUMPTIONS ..................................................................................................... 11
   Foreign Exchange and International Real-time Payments ..................................................... 11
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION ..................................... 13
   INITIATION ............................................................................................................................ 13
   AUTHENTICATION ............................................................................................................... 17
   PAYER AUTHORIZATION ...................................................................................................... 19
   APPROVAL BY THE PAYER’S PROVIDER .......................................................................... 21
   CLEARING ............................................................................................................................. 22
      Trusted Settlement System (TSS) ....................................................................................... 23
      Process Flow for Clearing, Settlement, Receipt (notification) and Reconciliation .............. 24
   RECEIPT ................................................................................................................................. 29
   SETTLEMENT ......................................................................................................................... 29
   RECONCILIATION .................................................................................................................. 30
PART A, SECTION 2: USE CASE DESCRIPTION ..................................................................... 31
   B2B Use Case ......................................................................................................................... 31
   B2P Use Case .......................................................................................................................... 34
   P2B Use Case .......................................................................................................................... 35
   P2P Use Case .......................................................................................................................... 37
PART A, SECTION 3: USE CASE BY EFFECTIVENESS CRITERIA ....................................... 38
PART B: BUSINESS CONSIDERATIONS ................................................................................. 40
   IMPLEMENTATION TIMELINE ............................................................................................... 40
   VALUE PROPOSITION AND COMPETITION ....................................................................... 43
      Value Proposition .............................................................................................................. 43
Competition.......................................................................................................................... 44
INTEGRATION EFFORT.............................................................................................................. 45
  B2B Use Case .......................................................................................................................... 45
  P2B Use Case .......................................................................................................................... 45
  B2P Use Case .......................................................................................................................... 46
  P2P Use Case .......................................................................................................................... 46
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA ................................. 47
  UBIQUITY.............................................................................................................................. 47
  EFFICIENCY........................................................................................................................... 49
  SAFETY AND SECURITY ....................................................................................................... 51
  SPEED (FAST) ....................................................................................................................... 54
  LEGAL FRAMEWORK ........................................................................................................... 55
  GOVERNANCE ...................................................................................................................... 57
ADDENDA.................................................................................................................................. 58
  Addendum A ........................................................................................................................... 59
THE INTERCOMPUTER INTEROPERATING SYSTEM (IC IOS) ............................................. 59
  Hosted / Distributed Architecture ......................................................................................... 59
  Digital Identities and Authorities ......................................................................................... 59
  ANSI/ITU/ISO Object Identifiers (OIDs) Make InterComputer a Registration Authority . 60
  The Secure Interface Device (SID) ....................................................................................... 61
  Installation Process ................................................................................................................ 62
Addendum B ............................................................................................................................ 64
INTERCOMPUTER INTEROPERATING SYSTEM (IC IOS) PATENT CLAIMS .................. 64
Addendum C ............................................................................................................................ 67
THE INTERCOMPUTER NETWORK LEGAL FRAMEWORK ............................................. 67
Addendum D ............................................................................................................................ 68
  CENTRALIZED ARCHITECTURE, NETWORK OPERATIONS, SECURITY AND
  EFFICIENCY ............................................................................................................................ 68
Addendum E ............................................................................................................................ 70
DIRECTORY STRUCTURE ........................................................................................................ 70
Addendum F ............................................................................................................................ 71
THE BIG PICTURE OF THE RISK ENVIRONMENT .............................................................. 71
EXECUTIVE SUMMARY


While ubiquitously accessible via personal computer, tablet, or smartphone, the InterComputer Network (ICN) does not rely in the least on voluntary human compliance with published standards. Neither does it rely in the least on grossly unsecure technologies, particularly the World Wide Web protocols. The InterComputer Network is the antithesis of “open source” software.

The ICN is built on the InterComputer InterOperating System (IC IOS). The IC IOS is standardized software. This means 85-90% of any IC IOS installation is standardized. The remaining 10-15% of an installation is mapping client applications to the IC IOS. The IC IOS has been designed for straightforward customization to meet individual organizational requirements.

InterComputer software discussed in this proposal is covered by Full Utility U.S Patent No. 8,380,622 B2. The patent is entitled “Secure Electronic Payments with Reconcilable Finality” and is valid through 2026. Claims 1-12 and their respective sub claims are attached hereto in Addendum B. The claims will be cited specifically throughout this proposal by claim number.

The ICN completely eliminates all of the following gaps in current legacy payment systems:

1. **Clearing and settlement delays** – Legacy systems currently impose inherent delays in funds availability, typically several days. The ICN provides both an insured-secure path and a comprehensive legal framework for the execution, clearing, and settlement of electronic payments in real-time. This process is detailed in Patent Claims 1 and 7 as listed in Addendum B.

2. **Settlement Risk** – In like manner, the ICN eliminates settlement risk by automatically confirming sufficient funds before the transaction is initiated and immediately executing a non-repudiable, legally final transaction in real-time. These features are not optional, but are inherent in every payment made using InterComputer’s solutions. Our patent and software support a binding legal payment framework comprising contractual agreements between banks and their customers and between banks and other banks. This process is detailed in Patent Claims 1 and 7 as listed in Addendum B. (S.1)

3. **Systemic Risk** – Systemic technological risks in electronic payment systems have three primary sources:
The inherently unsecure nature of the message pathways employed

The relative ease with which user identity/authority credentials can be abused for fraudulent/criminal purposes

The necessity of manual human intervention to complete some transactions, especially when multiple legacy systems must be used for one transaction (S.1)

The ICN eliminates the severe, inherent risks of the World Wide Web protocols (http, https, ftp, ftps, etc.) by simply refusing to use them or be accessible to them. Instead, InterComputer applies multiple layers of patented, underwritten security technologies to the TCP/IP protocols of the Internet to guarantee secure message delivery. These layers include abuse detection, microburst tunneling, potential abuse detection, and continuous machine and data audit, and identity/authority management. These technologies comprise the IC IOS, on which all InterComputer payment solutions are built. Regardless of where the IC IOS servers are hosted, the ICN is inherently composed of fully insured “nodes of equal strength”. There is no “weak link” in the ICN chain. The IC IOS is more fully described in Addendum A of this document.

The IC IOS was entirely developed using a risk-evaluated methodology to CMMI quality standards in a single, secure environment for the sole purpose of earning underwritten transaction insurance (including the payment face value) for a ubiquitous, real-time electronic payment system. This unique coverage was achieved by driving the systemic risk of failure or loss so low that the remaining residual risk could be profitably eliminated through underwritten insurance at a nominal rate.

User identity and authority management are accomplished using a proprietary, enhanced version of X.509v3 digital certificates. It is enforced by a compelled three-factor authentication process including possession, knowledge, and biometric testing. This process makes the abuse of credentials stolen by keystroke logger or screen scraper (as in the recent cyber heist at the Central Bank of Bangladesh) impossible. Aliases of any kind are impossible within the InterComputer Network.

Banks and their customers must be enrolled before using the ICN to execute payments. This enrollment involves two contracts: one between InterComputer and the bank, and the other between the bank and its customer. This PL Payment Legal Network is part and parcel of the software and hardware components of the ICN, and is described in Addendum C of this proposal document.
InterComputer possesses two (2) unique, registered OIDs (Object Identifiers) Issued through ANSI, and has registered them with the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization (ISO). OIDs are values used to uniquely identify objects within the X.500 infrastructure, such as in Directory Services and X.509v3 digital certificates. The X.509 Standard requires OIDs in all digital certificates, in order for the certificates to be used correctly and comply with the standard. InterComputer has successfully registered OIDs which makes InterComputer the Registration Authority (RA) for all OIDs deeper within the tree. InterComputer’s registered OIDs will be used for the InterComputer Corporate Certificate Authority (CA) for user IDs, and those OIDs can be used by ICs servers and embedded into all digital user certificates that it creates.

An ICN member bank will install the IC IOS and map its customer account systems to the IC IOS appropriately. The bank also installs the ICN’s Trusted Settlement™ application on its transaction system. Doing so enables the bank to conduct real-time ICN transactions with any other bank on the ICN.

The member bank will then enroll its customers as ICN users (the enrollment process is detailed in Addendum A of this proposal). This process, performed via a feature called the ICN Control Bridge, is described in a subsequent section of this document. As enrolled users, customers will possess enhanced X.509v3 digital identity/authority certificates which will be used in a three-factor authentication process for each ICN transaction. In like manner, ICN member organizations may enroll their employees via the Control Bridge.

Enrolled users may install the ICN user interface app (aka PrivateLine™) on their smartphone, tablet, or PC. Business users may wish to connect their accounting/purchasing systems to the IC IOS via mapping or a pre-packaged plug-in from InterComputer. This will enable the initiation of PL Payments directly from their preferred business applications.

*With these pre-requisites satisfied, any registered user may initiate a real-time electronic payment.*

One typical user experience would be:

1. A Payer desires to securely pay a Payee for an item. Both the Payer and the Payee are enrolled ICN members via their respective banks.
2. The Payer starts the PrivateLine app on his/her smartphone and begins the three-factor authentication sequence: (Patent Claims 2,8)
a. Possession of the smartphone guarantees presence.
b. The entry of a passphrase and how it is entered guarantees knowledge.
c. The swipe of a fingerprint guarantees biometric identity.

3. The PrivateLine feature employs an out-of-band confirmation signal as part of the authentication process.

4. Once user identity and authority limits have been authenticated, the Payer selects the Payee, the payment amount, and enters/attaches any desired information pertaining to the transaction.

5. The Payer then initiates the actual payment and is presented with two successive disclaimer/warning/confirmation screens. Once the user confirms his/her approval of the payment twice, the ICN initiates the real-time payment process. This process, which is detailed below, routinely concludes in 10-15 seconds. It includes:
   - The secure transfer of all transaction messages
   - The automated application of all applicable regulations and corporate policies
   - Instant verification of sufficient funds
   - Pertinent transaction status messages sent to all parties
   - Archival of all transaction information for regulatory compliance
   - Legally final and binding settlement and clearing

Once concluded, the PL Payment is legally final, settled, and cleared, and is NOT repudiable. The funds received in the Payee’s account are immediately “good”. All PL Payments are “pushed”, not “pulled.”
## 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>The solution enables large, medium and small business to interconnect with each other through the complete purchase-to-payment process. PL Payments can be initiated from within treasury management or accounting systems, or through bank PrivateSites if mapped systems are unavailable. If organizations large or small authorize mobile devices to be used for payments, PL Pay supports this scenario. B2B includes any G2B and B2G payments. Remittance can be ordinary remittance data or actual forms with or without embedded xml data. Many large entities have mid-size and small business vendors and customers. IC already has QuickBooks and Sage 50 mapped using ISO 200022 xml syntax. Mapping to the large ERP providers and custom accounting systems is a matter of process. Remittance data travels two ways: 1) If business partner systems are mapped, directly posted between each other; 2) through payee banks with encrypted remittance and forwarded by the bank to their customer for decryption and use.</td>
<td></td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>Businesses can send payments in real time with recipients receiving notification via mobile phone or bank PrivateSite that a payment was made.</td>
<td>B2P payments include a note field for remittance or other contextual data.</td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>Users can pay business at point of sale or online using the PL Pay feature of the IC IOS protected mobile phone. They can also pay through an organization’s PrivateSite to</td>
<td></td>
</tr>
</tbody>
</table>
### Supported use case coverage summary

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>Supports individual payment between each other via mobile device or PC.</td>
<td>A substantial note field is available to include messages. The note information is not transferred to the bank with the payment instruction, the KMI of IC IOS enables the note to be attached to the payment through ICN.</td>
</tr>
</tbody>
</table>

### Cross-border Use Case Coverage

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

<table>
<thead>
<tr>
<th>Cross-border use case coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Case</strong></td>
</tr>
<tr>
<td>Business to Business (B2B)</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
</tr>
</tbody>
</table>
PROPOSAL ASSUMPTIONS

Foreign Exchange and International Real-time Payments

InterComputer’s software design includes real-time, cross-border payments in all use cases. Indeed, Lloyds has underwritten InterComputer’s eComprehensive Transaction Insurance globally. The same unique Transaction Insurance is now available from U.S. insurers as well. But the software has not been deployed or tested in an international setting with a foreign exchange (FX) component.

The provisioning/registering of users and the payment clearing/settlement process are the same.

The difference with InterComputer’s inclusion of FX in the near future is adding the foreign exchange price/bank decision during the payment initiation process.

There are two methods InterComputer will deploy:

1. Near to Mid-term
   a. InterComputer has established a relationship with major provider of FX pricing and bank options which will be integrated with PL Pay through a non-web API.
   b. FX enabled customers, individual, small, medium or large business will select a currency quotation as the last part of the sequence for entering a PL Payment.
   c. Payers have a 10-minute window to select from an array of quotations.
   d. The same payment acceptance screens as described in the payment process section of the proposal template apply.
   e. The TSS system debits the Payer bank account in real-time and credits a special InterComputer bank account at each bank executing the FX payment instructions.
   f. The FX mechanism of the participating banks is currently SWIFT. This means a 2-3 day period before the exchanged funds reach the foreign bank of the foreign bank customer utilizing InterComputer PL Pay system.
   g. The implementation timeline for this option is six months.

2. Mid-term to Permanent
   a. Over time, InterComputer intends to establish direct banking relationships with global banks to utilize TSS (which includes intermediaries as long as needed) for direct, insured-secure, real-time payments to occur.
   b. Steps c-g listed above are identical except for a modification in step g.
   c. For clearing and settling foreign funds, the TSS system debits the bank customer’s bank account in the amount required to cover the FX conversion. The International TSS system moves the money to the destination bank and bank
customer account in the expected currency and can manage the entire series of payment message debits and credits in less than one minute.

d. The implementation timeline for this option is dependent upon the willingness of the international banks involved.

The advantages of real-time international payment are speed and cost. This paradigm alters current FX purchase, clearing, and settling arrangements by reducing exchange costs and possibly eliminating the need for some current clearing/settling mechanisms.

There is no need for banks working in FX to place large cushions in their prices to cover settlement risk. Prices and quotations can be very close to actual. Large swings in currency valuations in an hour, day, or two to three days do not affect real-time international payments.

All banks and bank customers still enjoy the full security of the IC IOS and PL Pay along with end-to-end Transaction Insurance, should something go wrong. Since the Transaction Insurance is global, all parties to a transaction enjoy the insurance protection.
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

This section is covered by U.S. Patent 8,380,622 B2 – Claims 1,2,3,4,5,6,7,8,9,10,11,12.

Please refer to the Addenda for additional information regarding the standardized InterComputer InterOperating System or IC IOS.

INITIATION


Bank and customer enrollment is governed by the PL Payment Legal Network, which is described in Addendum C of this proposal document. Banks may enroll their customers (and organizations their employees) via the ICN Control Bridge application of the IC IOS, which is hosted and controlled by the bank or organization. During enrollment, banks and organizations may set limits on which accounts are authorized for ICN transactions, set limits on allowed transaction types, frequencies, face values, etc. (E.1.3, S.7.3) These user authority limits are included in enhanced X.509v3 digital identity/authority certificates generated by the enrollment process, which must be used to authenticate every ICN transaction. (S.7.1)

InterComputer possesses two unique, registered OIDs (Object Identifiers) issued by ANSI, which are registered through the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization (ISO). OIDs are values used to uniquely identify objects within the X.500 infrastructure, such as in Directory Services and X.509v3 digital certificates. The X.509 Standard requires OIDs in all digital certificates, in order for the certificates to be used correctly and comply with the standard. Since many companies use an OID, these values must be recognizable by others as true globally unique values.

U.S. law requires that ANSI maintain a record of all OIDs registered within the joint-iso-itu-t (2) arc. Thus, ANSI provides all registration services for the joint-iso-itu-t (2) arc.

InterComputer’s first registered OID makes InterComputer the Registration Authority (RA) for all Certificate Authorities (CAs) deeper within the tree. InterComputer’s second registered OID will be used by all Certificate Authorities (CAs) below InterComputer to mint digital certificates for use on the ICN.

Each ICN identity/authority certificate is absolutely unique. A user may only conduct transactions using the bank accounts authorized by the certificate. Therefore, an employee
wishing to use the ICN to conduct transactions using his personal bank accounts may NOT use the identity/authority certificates issued by his employer to do so. Instead, he must obtain separate identity/authority certificates from his personal bank for his personal accounts.

Enrollment enables banks, organizations and individual users to conduct transactions with any other bank, organization, or user enrolled in the ICN, subject to bank/organization policies and applicable laws. (U.1.2)

An ICN-enrolled user must install the ICN user interface on the device they use to make payments. This UI is called the PrivateLine™ app. PrivateLine is a standardized UI, which in part replaces the browser function to view and interact with ICN PrivateSites™ on the ICN. PrivateLine also contains secure applications such as tMail (Trusted Mail), tChat, Contextual Chat, and other useful apps. (U.4.1) PrivateLine features also include PL Pay™ and eCash™. PL Pay is the end user software component for use by bank customers for all use cases. Bank-branded PrivateSites can also be accessed via PrivateLine for additional insured-secure payment options. Bank customers can initiate payments in these ways:

1. PrivateLine “PL Pay” mobile or PC option.
2. PrivateLine “PL Pay eCash” mobile only option.
3. PrivateLine Bank PrivateSite option – Within the bank PrivateSite, PL Payments are accessible. Can be used via mobile, PC, or workstation.
4. PL Pay mapped to accounting, treasury management, or other ERP systems. (U.4.2) PrivateLine Contextual tChat and other tools are operative in mapped implementations.
5. PrivateLine “PL Pay” provides contextual data capabilities in all use cases.

In a typical user experience, a Payer selects a Payee name manually or with a search option from their authorized payee list. The Payee name is either an individual or an organization. The Payee’s name is the only characteristic required to identify the Payee on the ICN. (U.2.2)

The payment amount can be set several ways:

- Payer enters the payment manually.
- Payer’s device receives the amount by ICN PoS transmission.
- Payer’s device receives the payment amount from an ICN-enabled mapped application. (U.1.6, U.4.2)
- Payer’s device receives the payment amount through their bank’s ICN PrivateSite™ (a secure site not exposed to the World Wide Web).

The Payee is then presented with a summary of the payment information:

- Date/time of transaction.
In Pursuit of a Better Payment System

Faster Payments Task Force

- Organization, merchant, or individual to whom payment is to be made.
- Amount to be paid.
- A field describing invoice, account number, restaurant check, merchant checkout list and/or total, or other notes if applicable. (U.4.1)
  - (Note: The contextual data described at this point is not the extensive remittance data as part of B2B transactions, or specific contextual data for each use case.) (U.4.2)
    - If a P2P payment, some personal note may be used.
    - If a P2B payment an account number or invoice number may be used.
    - If a P2G payment a TIN or form number, time period, or other description can be entered.
    - If a restaurant check is presented, the user checks an “Add Tip” box which adds the ability to itemize a tip and increase the payment amount.

The payee reviews the payment data and presses the “Make Payment” button. (U.2.4) (Patent Claims 1, 7)

At this point, the payee sees a screen with legal language detailing their agreement with their bank that the incipient PL Payment is final and cannot be rescinded or repudiated.

The Payee then clicks or presses the “Confirm Payment” button associated with the short legal acceptance language. Once the “Confirm Payment” button has been pressed, the transaction message is stored in the bank customer’s payment record in ICN database associated with the Payee on the Payee side of the IC IOS.

The Payee is then presented with another screen with the short legal acceptance language as stated above. The Payee then presses the “Send Payment” button. (U.3.2) At this point the payment instruction is sent to the bank, immediately initiating the following process:

1. A feasibility message is sent to the Payee’s bank to verify sufficient available funds for the payment.
2. An acknowledgment message is returned to the user notifying the PL Pay System that the ICN can or cannot proceed with the payment.
   a. If funds are not available, the payee receives a message with as part of the acknowledgment message that adequate funds or associated bank overdraft agreement, or other credit line is not available. The payment cannot proceed.
   b. If during the provisioning process, the bank and its customer can specify a hierarchy of accounts to be used for making payments. If funds in one account are inadequate, and funds in another account are adequate the payment moves forward on that pre-determined basis.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
INITIATION EFFECTIVENESS CRITERIA ASSESSMENT

U.1 (Accessibility) – The ICN is currently very effective at satisfying criteria U.1.1, U.1.2, U.1.4, U.1.5, and U.1.6. The ICN is effective at satisfying criterion U.1.3 (see Assumptions section above).

U.2 (Usability) – The ICN is currently very effective at satisfying criteria U.2.1, U.2.2, U.2.3, and U.2.4.


U.4 (Contextual data capability) – The ICN is currently very effective at satisfying criteria U.4.1, U.4.2, U.4.3.

U.5 (Cross-border functionality) – The ICN is currently effective at satisfying criteria U.5.1 through U.5.5

U.6 (Applicability to multiple use cases) – The ICN is currently very effective at satisfying criteria U.6.

E.4 (Payment format standards) – The ICN is currently very effective at satisfying criteria E.4.1, E.4.3, and E.4.4. The ICN is currently somewhat effective at satisfying criterion E.4.2. The ICN is not now, never has been, and never will be effective at satisfying criterion E.4.5 because doing so is antithetical to the insured-secure nature of the ICN. If something goes wrong with a PL Payment, transaction insurance covers the loss in full. What do you think would happen when something goes wrong with your payment made on a transparent, open source system published by a standards development organization?

S.7 (Security controls) – The ICN is currently very effective at satisfying criteria S.7.1, S.7.2, and S.7.3.

S.9 (End-user data protection). The ICN is currently very effective at satisfying criteria S.9.1, S.9.2, and S.9.3.
AUTHENTICATION

InterComputer utilizes a strong but straightforward three-factor authentication process. Three-factor authentication, when properly deployed, is 99.999% reliable. (S.7.1, S.7.2) The three factors are:

1. What you know. (user name, password) (S.7.1)
2. Who you are. (biometric device integrated with IC IOS enabled smartphone or mobile device) (S.7.1, S.7.2)
3. What you have. (Secure Interface Device in connection with smartphone or mobile device.) (S.7.2)

As described in the previous section on Initiation, enrolled ICN users receive individual, signed X.509 v3 digital identity and authority certificates in a hierarchal chain. The bank will use the ICN Control Bridge app to generate two public-private key pairs for each customer. In like manner, an organization may do so for its employees. Small organizations may optionally request that InterComputer generate key pairs for their employees. All private keys are protected by InterComputer’s proprietary methods. Even though the IC Control Bridge creates public-private key pairs, only the public keys are shared while the private keys remain separated from the system. (S.7.1, S.9.1, S.9.2, S.9.3, S.10.1, S.10.4, S.10.5)

Each ICN identity/authority certificate is absolutely unique. A user may only conduct transactions using the bank accounts authorized by the certificate. Therefore, an employee wishing to use the ICN to conduct transactions using his personal bank accounts may NOT use the identity/authority certificates issued by his employer to do so. Instead, he must obtain separate identity/authority certificates from his personal bank for his personal accounts. (S.7.3)

Within banks and other organizations, the enhanced X.509v3 identity and X.509v3 authority certificates are signed in a proprietary, hierarchal method which not only authenticates an individual or employee, but points back to whomever authorized that individual or employee to engage in payment activity. This creates a “chain of command” for subsequent use in audits or other forensic activities. (S.7.3, E.7)

The ICN uses the three-factor login requirements to validate each individual identity certificate AND the corresponding authority certificate. All validation messages and acknowledgement messages create two-way, full duplex digital communications at all times. Other proprietary layers of protection continuously operate on these messages to strengthen security and continuously monitor message traffic across the TCP/IP connections within the ICN. Every ICN transaction uses the same messaging pattern and sequence. Should any problem or deviation be
detected in the messaging pattern, the message stops and is automatically re-routed by the IC IOS until it is successfully validated. Should a message stop for any reason, alerts, reports and logs are sent to designated bank employees for analysis. (S.7.1)

In short, the connection between the user’s device and the bank is secured by multiple layers of protection and multiple layers of encryption. Once the identity and authority certificates are validated/authenticated, the required acknowledgment message is returned to the user’s device PL Pay App that sufficient funds are available and the payment proceeds no further intervention and/or interruption. (S.7.1, S.7.2, S.10.6)

**AUTHENTICATION EFFECTIVENESS CRITERIA ASSESSMENT**

U.2 (Usability) – The ICN is currently very effective at satisfying criteria U.2.1, U.2.2, U.2.3, and U.2.4.


S.7 (Security controls) – The ICN is currently very effective at satisfying criteria S.7.1, S.7.2, and S.7.3.

S.9 (End-user data protection) – The ICN is currently very effective at satisfying criteria S.9.1, S.9.2, and S.9.3.

PAYER AUTHORIZATION

During Authentication (step 2 of the transaction process), Payer Authorization (step 3 of the process) occurs simultaneously in the ICN. InterComputer refers to the functions of “Authentication” and “Payer Authorization” as a single process called “Validation.” The authorization for individual accounts is defined by the relevant bank policies. The digital authorities must align with the bank’s customer account system perfectly before the PL Payment instruction can move forward.

Organizations generate the ICN identity and authority certificates for their individual employees. These authorities may include limits such as which organization accounts an employee may utilize on the ICN, any transaction limits which may apply (such as face amount, payment frequency, geographic restrictions, etc.), or any secondary signatures required to authorize a transaction. The certificate authorities will be validated by the bank for each PL Payment instruction, and must match the bank’s permissions and authorities, which we were mapped during the IC IOS installation at the bank. S.9.1, S.7.1, S.7.3.

The electronic opening and closing of accounts are legitimate authority options because of the insured-security of the system. In the individual account use case, when the authority certificate is minted, the bank employee’s digital certificate electronically signs the individual customer’s digital certificate. The bank employee certificate points back to the chain of authority at the bank which authorized the bank employee to open the account and/or change authority limits.

If an employee’s organizational role, tasks, or authorities regarding payments authorities change, the organization can use the IC Control Bridge to generate a new authority certificate containing the new role(s), tasks, mini-roles and mini-tasks. The existing authority certificate is automatically revoked upon generation of the new certificate. The authority attributes in the new certificate must be identical to the bank account attributes at the related bank. S.9.1.

An ICN validation server at the bank operations center (or at a secure IC facility) contains the identities and authorities users have in connection with the bank accounts. The validation server compares the identity/authority certificate signed with payment instruction to those contained in the validation server. When both identity and authority are validated, and the acknowledgment is returned to the user’s mobile device, PC or workstation, the payer authorization process is complete. S.7.2, U.2.1, U.2.2, U.2.3

The validation process, from Payer feasibility request to bank acknowledgement, occurs in fewer than five seconds. A successful feasibility request immediately moves the payment transaction to the funds movement, clearing/reconciliation, and legally final settlement process.

In summary, the authentication process is:
1. After the validation step is completed and sufficient funds availability is verified, the payment request is sent to the bank’s validation server. Here, the identity and authority certificates are validated against the public key in the bank validation server.

2. The payment instructions are immediately sent to the Trusted Settlement System (TSS) for execution. The entire authentication process takes five seconds or less.

3. This process seemingly operates in the background unless something in the authentication/validation process is not correct. If an error occurs, an alert or message is sent to a designated employee and a designated bank employee monitoring the TSS system at the bank. If there has been any change on either side, validation cannot occur and the transaction is immediately halted. S.9.2

An authenticated user may pre-authorize one or more payments and set the parameters of those payments (e.g. bank account, amount, date and time, frequency, etc.). The Validation process described above applies equally to both real-time and pre-authorized payments. S.2.1, S.2.2, S.2.3

PAYER AUTHORIZATION EFFECTIVENESS CRITERIA ASSESSMENT

U.2 (Usability) – The ICN is currently very effective at satisfying criteria U.2.1 through U.2.4

U.3 (Predictability) – The ICN is currently very effective at satisfying criteria U.3.1 through U.3.6.

S.2 (Payer authorization) – The ICN is currently very effective at satisfying criteria S.2.1 through S.2.3

S.7 (Security controls) – The ICN is currently very effective at satisfying criteria S.7.1 through S.7.3

S.9 (End-user data protection) – The ICN is currently very effective at satisfying criteria S.9.1 through S.9.3.
APPROVAL BY THE PAYER’S PROVIDER

The feasibility acknowledgment message described above indicates to the user’s device that sufficient funds are available for the payment. The payment message is then signed by the digital certificate from the bank or bank branch and sent directly to the clearing step of the process with no further interaction or interruption. The payment instruction triggers InterComputer’s Trusted Settlement System (TSS) for clearing, reconciliation, settlement, funds transfer and final reconciliation as described in steps 5, 6, 7, and 8 below.

PAYER’S PROVIDER APPROVAL EFFECTIVENESS CRITERIA ASSESSMENT

S.3 (Payment finality) – The ICN is currently very effective at satisfying criteria S.3.1, S.3.2, and S.3.3. PL Payments are not repudiable, but are fully insured for the face value. The Legal Framework governing payment finality is explained in detail in the next section of this proposal.

S.7 (Security controls) – The ICN is currently very effective at satisfying criteria S.7.1 through S.7.3.

S.9 (End-user data protection) – The ICN is currently very effective at satisfying criteria S.9.1 through S.9.3.

F.1 (Fast approval) – The ICN is currently very effective at satisfying criteria F.1. The interval from the completion of payment Initiation (just following Payer Authorization to their Provider, or just following confirmation by the Payer’s Provider that pre-authorization exists for a given payment) to the point when the Payer’s Depository Institution or Regulated Non-bank Account Provider approves or denies the payment is less than 10 seconds for PL Payments.

F.5 (Prompt visibility of payment status) – The ICN is currently very effective at satisfying criteria F.5.1 and F.5.2.
CLEARING

The fact that the ICN is a real-time payment system means that Steps 5 through 8 (Clearing, Receipt, Settlement, and Reconciliation) occur either simultaneously or within seconds of each other. Therefore, Steps 5 through 8 are detailed together below. These steps are all executed within the Trusted Settlement System (TSS) previously described, and detailed in Addendum A of this document.

Data formats for payment and applicable contextual data are in ISO 20022 xml syntax as they apply to each step. (U.3.3)

Steps 5 through 8 are all covered by all claims in InterComputer’s Patent 8,380,622 B2, Secure Electronic Payments with Reconcilable Finality. These claims are listed in Addendum B of this document.

Steps 5-8 are integrated with, and governed by, the PL Payment Legal Network. (L.1, L.2, L.3, L.4, L.5) The legal framework is interlinked with the TSS software and its language appears at the appropriate points in the process of executing steps 5 through 8. The PL Payment Legal Network has been approved by insurance underwriters providing Transaction Insurance coverage from end-to-end against any form of cybercrime. This coverage includes the value of the money in the transaction. This one-to-many contract authorizes each bank to establish a correspondent bilateral TSS account relationship with every other bank signatory to the TSS agreement. Since all real-time payment activity occurs within the TSS, any bank transacting payments with any other bank has access to all of the information associated with those transactions. (E.1, S.11)

Multiple layers of protection are operative throughout the entire messaging process from end-to-end. (E.5) These layers of protection are:

1. All messages are electronically signed by enhanced X.509 v3 digital identity certificates. When the term “signed” is used, it means signed by the Payer’s unique enhanced X.509 v3 digital identity certificate.
2. Contextual Data can be transmitted two ways on ICN. If a direct mapping relationship exists, the payment instructions are presented to the bank’s TSS system for real-time processing. If direct mapping relationships do not exist, customers can send contextual data through the TSS system with separate encryption to keep contextual data private.
3. Continuous audit is operative in end-to-end message movement.
4. Microburst Tunneling™ constantly compares all messages and their corresponding acknowledgements. Payment data is not moved until the microburst tunnel is established. A detection mechanism notifies the system if there is any change in the
message/acknowledgment tunnel. In that case, the system shuts down the tunnel and re-routes it until the encrypted data arrives safely at its correct destination.

5. Abuse Detection enables rules which are applied to all messages. If an abuse rule detects a problem, the message stops and alerts are sent to the appropriate parties.

6. Potential Abuse Detection monitors messages for anomalies. It does not shut down the message movement, but is noted and reported to appropriate designated parties to determine if the anomaly is reasonable or whether it should be added to the abuse rules.

**Trusted Settlement System (TSS)**

(This section is covered by U.S. Patent 8,380,622 B2 – Claims 1 through 12, inclusive.)

TSS performs all clearing, settlement, and reconciliation functions in real-time with full legal finality. (S.3) Two banks may use TSS to clear, settle, and reconcile payments between themselves without involving a third party clearing service (Patent Claims 1, 2, 3, 4, 7, 8, 9, 10). Alternatively, the Federal Reserve (Patent Claims 7 and 12) or a third party clearing service (Patent Claims 5 and 10) may host TSS to provide these services to banks.

TSS operation is governed by the PL Payment Legal Network, which is described in Addendum C of this proposal document. (S.11) Each bank enrolled in the ICN signs the same enrollment agreement. It is a one-to-many contract that establishes three foundational obligations:

1. Authorization to establish an auditable ICN direct correspondent bank account with every other bank on the system.
2. The bank agrees that every completed PL Payment is legally final, binding and non-rescindable.
3. The bank agrees to bind their customers to the same terms and conditions, i.e., the “legally final” non-rescindable attribute of PL Payments.

These legal terms and conditions are established with every customer ICN enrollment (by contract between the bank and its customer) and reaffirmed with every PL Payment instruction. Every time a customer makes a PL Payment, these terms and conditions will be presented and must be actively acknowledged and accepted **twice** by the customer prior to payment execution. (U.3.2)

This authorization is filed in the IC IOS database associated with the Payer.

The previously authenticated and Payer bank-approved payment message is received by The TSS. This triggers a series of debits, credits, and notifications, which must always match and reconcile. In other words, an “in-balance” condition is continuously required through the payment process on an item by item basis or the payment stops instantly.
Process Flow for Clearing, Settlement, Receipt (notification) and Reconciliation

Note: The following steps presume the TSS is already mapped to banks’ customer account systems at the sending and receiving banks. Signed acknowledgment messages are returned with every initiation message throughout the cycle. The actual money does not “move” between banks until all payment instructions, corresponding acknowledgements, and a “perfectly in-balance” condition exists. In the final step the debit and credit are then applied simultaneously to move the money between banks. The payment is then cleared, settled and legally final and binding. The actions in the sequence have already been authorized by the IC Bank Agreement. (This process flow does not examine or impact internal bank accounting system actions as debits and credits are applied to customer accounts.)

Complete PL Payment Process Flow Summary

1. The payment instruction from the Payer to the Payer Bank is signed by the digital certificate of the Payer, and validated by the bank validation server (U.2, U.3)
2. A payment “feasibility query” is made to the Payer bank account. A signed bank acknowledgement message is returned to the Payer’s PL Pay system. If the funds are not available, the Payer is so notified. The payment cannot move forward.
3. If funds are available, the TSS at the Payer Bank acts as follows:
   a. A Debit (DR) entry is applied to their customer’s bank account in the amount of the payment.
   b. The TSS enables the Payer Bank to generate and digitally sign an offsetting Credit (CR) payment entry in the amount of the payment to the Payee Bank’s TSS correspondent account held at the Payer Bank.
   c. A signed notification is sent to the Payee Bank through the TSS. Acknowledgement of the notification prompts the next stage of entries.
   d. A Debit (DR) entry is applied to the Payee Bank’s TSS correspondent account held at the Payer Bank’s TSS.
   e. A Credit (CR) entry is applied to the Payer Bank’s TSS correspondent account at the Payee Bank.
   f. A Debit (DR) entry is applied to the Payer Bank’s TSS correspondent account at the Payee Bank. Prior to the final Credit to the Payee Bank customers account and notification forwarded to the payee.
      i. At this point all signed messages carrying payment information have been acknowledged, with Debit (DR) and Credit (CR) entries applied to the appropriate accounts as though the funds have moved and are final.
ii. If, for any reason, an out-of-balance condition arises, or signed payment and acknowledgement messages do not compare perfectly, the payment stops and all parties are notified.

g. The final step to complete the real-time payment occurs when all debits and credits are in balance and all acknowledgement messages have been received.

4. The signed payment message, and corresponding signed acknowledgement message in the TSS, all provisional debits and credits throughout the process are permanently applied to the respective accounts in the payment cycle. The money has moved between the banks and the funds are settled. (S.4)
   a. All signed messages and signed acknowledgement carry balanced debit and credit entries. The provisional entries constitute clearing.
   b. The “in-balance” condition of all entries does exist which is end-to-end reconciliation.
   c. The unscathed signed messages and acknowledgments compare perfectly according to the microburst tunneling software.

5. An average of 10-15 seconds is required to reach this point. The funds are immediately available for re-use. (F.1, F.2, F.3, F.4, F.5)

6. The bank customer is then notified of the payment deposited to their account as the next automated sequence.
   a. The Payee Bank sends a signed notification message of the payment received to their customer’s PL Pay system. Related Contextual Data is also sent in the same time.
   b. The Payee Bank customer’s PL Pay system sends a signed acknowledgment back to the bank TSS. This is the last message the bank and their customer exchange on the payee side of the payment transaction.
      i. If the bank customer is using a mapped accounting system, the remittance information can be automatically posted to the A/R system.
      ii. Alternatively, the PL Pay System’s optional “holding bin” enables the incoming remittance to be reviewed and accepted by a designated employee. All automation can be subject to authorized human control.
      iii. If the bank customer does not have a mapped accounting system, the data file is converted into text format and sent for their customers use.
      iv. If the payee bank customer is an individual, contextual data such as notations etc., are sent in text format to the PL Pay System.
      v. If the bank customer requires a form for Contextual Data such as a government agency, the form data can be placed into xml format and forwarded as a form with usable xml data.
vi. An additional five seconds is needed to provide the notification of payment received with contextual data. If the contextual data file is very large, the time will be longer based upon ISP bandwidth, user Internet bandwidth and/or heavy Internet congestion.

7. Step 8 is labeled “Reconciliation”. Every bank on the Trusted Settlement System (TSS) can have full confidence that every payment is legally binding to their Payer and Payee customers. However, for audit purposes every bank can have authorized employees assigned to monitor, or if need be, interact with the real-time system. Any customer account on either side of the transaction can be viewed by total accounts, and drilled down to granular detail. Any single customer, bank account, and payment can be viewed with all Transaction ID’s, names, signed message proofs with the corresponding bank. Certainly random audits can occur, full reports, etc. from within the TSS. (E.7)

An example of the TSS Ledger associated with each payment follows:

**Trusted Settlement System (TSS) Ledger**

### Payment Feasibility Query

<table>
<thead>
<tr>
<th>Step No.</th>
<th>Payer</th>
<th>Payment Amount</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feasibility Request to Bank to Verify Funds Availability</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Payer Bank Acknowledge Funds Available Y/N</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If Payment Feasibility Query is Successful, the Payment Request Continues Uninterrupted

<table>
<thead>
<tr>
<th>Step No.</th>
<th>Payer and Payer Bank</th>
<th>Payment Amount</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Payer’s Instruction Sent to TSS at Payer Bank</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Bank Acknowledgement Returned to Payer PL Pay System</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Debit Applied to Payer’s Bank Account</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Credit Applied to Receiving Bank’s Correspondent TSS Account</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step No.</th>
<th>Payee Bank and Payee</th>
<th>Payment Amount</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Debit Applied to Sending Bank’s Correspondent TSS Account</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Credit Applied to Payee’s Customer Bank Account</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>Payment Complete, Cleared and Settled, Money Has Moved</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Payment Notification Sent to Payee’s PL Pay System</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>Contextual Data Sent to Payee’s With Notification to PL Pay System</td>
<td>N/A</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Optional Payer to Payee Activity if Payer and Payee have an InterConnection Directly On ICN

<table>
<thead>
<tr>
<th>Step No.</th>
<th>Payee and Payor Acknowledgment</th>
<th>Payment Amount</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Independent Confirmation of Payment ReceivedSent to Payer’s PL System</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>Contextual Data Transferred Between Systems vs. Going Through Banks</td>
<td>$10,000,000,000.00</td>
<td>Yes</td>
</tr>
</tbody>
</table>
If the Payer and Payee have subsequent grievances or issues between themselves concerning a particular payment, most reasonable people will take steps to settle their differences amicably. If the Payer and Payee cannot settle a payment issue, they have the court system to help them do so. The ICN relieves banks of the legal and management burdens associated with rescinded or repudiated payments. (U.3.5)

All banks have a choice of hosting their own TSS servers or having a third party do so. Smaller banks and credit unions may choose to have InterComputer host TSS on their behalf. InterComputer may also establish relationships with community bank and credit union software and service providers to perform this function on behalf of their existing bank and credit union customers. TSS operations are easily well within the typical technical expertise of any depository institution, large or small.

Regardless of where the TSS servers are hosted, the ICN is inherently composed of fully insured “nodes of equal strength”, all of them completely unexposed to WWW risk. There is no “weak link” in the PL Payment chain.

The following diagram shows the message flows for a payment cycle in the TSS, which normally completes in less than 15 seconds:
CLEARING EFFECTIVENESS CRITERIA ASSESSMENT

U.1 (Accessibility) – The ICN is currently very effective at satisfying criteria U.1.1 through U.1.6.

U.2 (Usability) – The ICN is currently very effective at satisfying criteria U.2.1 through U.2.4.

U.3 (Predictability) – The ICN is currently very effective at satisfying criteria U.3.1 through U.3.6.

U.6 (Applicability to multiple use cases) – The ICN is currently very effective at satisfying criterion U.6.

E.4 (Payment format standards) – The ICN is currently very effective at satisfying criteria E.4.1, E.4.3, and E.4.4. The ICN is currently somewhat effective at satisfying criterion E.4.2. The ICN is not now, never has been, and never will be effective at satisfying criterion E.4.5 because doing so is antithetical to the insured-secure nature of the ICN. If something goes wrong with a PL Payment, transaction insurance covers the loss in full. What do you think would happen when something goes wrong with your payment made on a transparent, open source system published by a standards development organization?

E.7 (Exceptions and investigations process) – The ICN is currently very effective at satisfying criteria E.7.1 through E.7.3.

S.4 (Settlement approach) – The ICN is currently very effective at satisfying criteria S.4.1 through S.4.3.

S.5 (Handling disputed payments) – The ICN is currently very effective at satisfying criteria S.5.1 through S.5.5. It should be noted that since all PL Payments are non-repudiable, a request from the Payer for a voluntary refund from the Payee is a simple, plain language message. Such a message can be sent by phone or text or e-mail, or by the ICN’s PrivateLine app. Regardless of the transmission mode, the message is not legally binding on the Payee and will never be seen by the TSS or by either bank involved in the original transaction. If the Payee chooses to “refund” the original payment, he can do so by initiating a new PL Payment of the same amount. Note, however, that the original payment and “refund” payments are not linked in any way within the PL Payment Legal Network. Neither bank, nor InterComputer, has any obligation to act regarding a “refund” of the original, legally final PL Payment.

S.6 (Fraud information sharing) – The ICN is currently very effective at satisfying S.6.1 through S.6.7 because the mere sharing of fraud information via a centralized repository has no effect on real-time payments. ICN’s digital identity/authority certificates, multiple layers of protection
(including abuse and potential abuse detection), TSS operations and full value transaction insurance all work together to prevent fraud in real-time. Should a number of incidents become sufficient to indicate a fraud pattern, any user’s digital credentials can be immediately suspended or revoked by the issuer to preclude any further incidents. (S.7.3) Sharing any generalized form of technological fraud information (beyond the identity of the perpetrator) with non-real time systems would have little to no value in preventing future fraudulent actions. The nature of the ICN makes all such information *sui generis*.

S.7 (Security controls) – The ICN is currently very effective at satisfying criteria S.7.1 through S.7.3.

S.9 (End-user data protection) – The ICN is currently very effective at satisfying criteria S.9.1 through S.9.3.

F.2 (Fast clearing) – The ICN is currently very effective at satisfying criterion F.2.

F.3 (Fast availability of good funds to payee) – The ICN is currently very effective at satisfying criterion F.3.

F.4 (Fast settlement among depository institutions and regulated non-bank account providers) – The ICN is currently very effective at satisfying criteria F.4.1 through F.4.3.

F.5 (Prompt visibility of payment status) – The ICN is currently very effective at satisfying criteria F.5.1 and F.5.2.

**RECEIPT**

The fact that the ICN is a real-time payment system means that Steps 5 through 8 (Clearing, Receipt, Settlement, and Reconciliation) occur either simultaneously or within seconds of each other. These steps are all executed within the Trusted Settlement System (TSS) previously described, and detailed in Addendum A of this document. Therefore, Step 6 (Receipt) is described in detail in section 5 above.

**SETTLEMENT**

The fact that the ICN is a real-time payment system means that Steps 5 through 8 (Clearing, Receipt, Settlement, and Reconciliation) occur either simultaneously or within seconds of each other. These steps are all executed within the Trusted Settlement System (TSS) previously described, and detailed in Addendum A of this document. Therefore, Step 7 (Settlement) is described in detail in section 5 above.
RECONCILIATION

The fact that the ICN is a real-time payment system means that Steps 5 through 8 (Clearing, Receipt, Settlement, and Reconciliation) occur either simultaneously or within seconds of each other. These steps are all executed within the Trusted Settlement System (TSS) previously described, and detailed in Addendum A of this document. Therefore, Step 8 (Reconciliation) is described in detail in section 5 above.
PART A, SECTION 2: USE CASE DESCRIPTION

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

B2B Use Case

Note: All use case descriptions utilize the same procedures at the point of payment initiation as described in Part A: Detailed End-to-End Payments Flow Description.

When discussing certain use cases, once individuals have a bank generated identity certificate, the underlying Key Management Infrastructure (KMI) enables fast, simple, interconnection at Points of Sale or with businesses where no prior relationship has existed.

B2B

Integrated Accounting Systems
1. A purchase decision is made.
2. The purchase order is generated, signed, and sent across the ICN to the seller side.
3. The seller’s system creates a sales order.
4. Should any question arise during this process, contextual chat is available so that each side can activate a tChat window in connection with the document and ask a question or correct an error. For example:
   a. Seller processes the sales order and notices a variance from a quotation.
   b. The seller activates a chat window with the document visible.
   c. If the appropriate person is at his or her workstation on the purchasing side, or whether they see it a later time, they can open the tChat window and see the document in understand the communication “in context.”
   d. The purchase side can respond in real-time or delayed time as the case may be.
   e. tChat is available during any stage of the transaction at any point in time, including after the payment has been made.
f. tChat messages are archived for later purposes if needed.
   i. Experience has shown that people are extremely polite in Contextual Chat communication since they know the tChat is archived with the document.

5. Once the seller ships the goods or performs the service, the accounting system generates the invoice and sends it across the ICN to the purchase side, either automatically or with manual approval as the seller prefers.

6. The A/R and A/P systems are automatically updated as the mapped data path enters the data automatically.

7. Payment of the invoice from the purchaser to seller occurs per agreed terms. Any invoice can be paid ahead of schedule date or time or delayed for flexibility when needed.

8. Once the payment is sent, it clears and settles in real-time per the clearing and settlement cycle described in Section A, Payment Cycle.

It is important to note that the IC IOS connection between the bank and its organizational customer can also initiate payment instruction to legacy payment systems such as ACH and Fedwire.

Also, the IC IOS connection between banks can transfer check images for real-time clearing and settling. It is confirmed by legal opinion that business checks are subject to the “finality” provisions of the IC bank and customer agreements. There is no contradiction with the Check Truncation Act of 2002. (Legal research still needs to be performed regarding consumer check images in connection with the Check 22. The images can be cleared and settled in real-time, but whether or not InterComputer’s legal agreement for legally binding finality conflicts with any provision of Check 22 has not been determined.)

The B2B Case is summarized in the following diagram:
Graphical flow diagram of the ICN PL Payments B2B use case.
**B2P Use Case**

Examples of real-time payments organizations can send to individuals include refunds and purchases such as an automobile dealer buying a car from an individual. Like B2B, the B2P use case enables contextual data to be sent with the payment in encrypted form. The PL Pay System or PrivateSite through which payment notification is sent will include the contextual data which will be decrypted and rendered in text and or other data formats as desired.
P2B Use Case

Note that P2B is broken down into two parts in this description because there are two distinct use sub-use cases; 1) A person paying any organization not at the Point of Sale; 2) A person paying an organization at the Point of Sale.

P2B Not at Point of Sale

An individual may make a real-time payment to an organization by:

1. PC-based, bank-branded or PrivateLine PL Pay System.
   a. Can be done through a bank PrivateSite
   b. Can be done through the PL Pay App UI
2. Mobile based payment initiation is done through the bank branded PL Pay app installed on a mobile device which is integrated with the IC IOS.

Once an online payment is made, the corresponding messages are sent out-of-band of the web and reaches the web retailer’s account along with the corresponding payment notification. This feature removes a large threat and constant flow of small and large web related fraudulent payment activity. Hackers cannot intercept the payment information or the payment instruction, neither can they steal financial information from a web-connected database.

Any organization, such as a utility or a government entity, can be paid P2B through the PL Pay app. It will be advantageous for the Payer to include account number, TIN, invoice number or other information relevant to correct crediting of “payment received” in the contextual data note field.

Another example of P2B from a PC is the potential remittance of a personal tax return with a payment. The tax return data can be parsed into xml data. The tax form can travel encrypted with the payment to U.S. Treasury or to a designated depository bank. The payment processes in real-time and data fields are mapped between the form and IRS systems accordingly. Federal tax deposits of various types can be initiated from integrated accounting apps, an IRS PrivateSite on the ICN, or through a mobile device. IRS customer account systems could be significantly upgraded by conversion to InterComputer Validation and Application servers.

Once the mobile P2B payment has been initiated, it follows the ICN clearing and settlement steps, which take approximately 10-15 seconds. The Payee bank updates their customer’s bank account balance, and sends a notification to the PL Pay app on the receiving smartphone or PC based PrivateLine PL Pay app. The bank branded PL Pay app for mobile device or PC provides access to the bank PrivateSite to access payment receipt and all other bank PrivateSite functionality offered.
The PL Pay app contains a note field to send contextual data with the payment. It may reference a purchase, loan, gift, or courtesy note. The recipient PL Pay app displays the note. The note is encrypted in a manner a bank cannot decrypt for privacy purposes.

**P2B at Point of Sale**

The Point of Sale capability of mobile devices is straightforward, streamlined, and effective. PL Pay Real-time payment instructions can be initiated through the NFC readers which many merchants are adding due to Apple Pay, Samsung Pay, and Android Pay. However, it is not required or necessarily the most comprehensive and safest way. All merchants and restaurants can be provisioned by InterComputer or their banks. Once provisioned to send and receive real-time payments, the merchant or restaurant can ring up a sale and submit the invoice, bill, check or total to the PL Pay App system as a presentment for the total due. This information is transmitted across the IC IOS from the establishment to the mobile device. (Remember they can form an interconnection on the fly.) All the merchant or restaurant needs is a smartphone or other device provisioned with PL Payments at the point of sale. The detailed total due appears in the individual’s PL Pay app on their mobile device. Once they review the bill, they send the payment as described in sections 1-8 of the payment cycle. There is also a “Tip” field in the PL Pay app for restaurant purchases. In this case, the Payer reviews the total due and has the ability to add a tip. A new total payment to send amount is shown and the modified payment is sent accordingly. The merchant then receives their payment in about 15 seconds.

Banks can provide added value to their customer through a PrivateLine app which provides for a record of purchases and storage of legal receipts. People will pay for the convenience of being able to produce a record or receipt of purchases at any time. This same feature can include budgeting and personal financial applications.
**P2P Use Case**

An individual may send money to another individual by:

1. PC-based, bank branded or PrivateLine PL Pay System.
   a. Can be done through a bank PrivateSite
   b. Can be done through the PL Pay App UI
      i. This is a configuration choice for the user.
      ii. The PL Pay UI is faster to initiate the payment.
2. Mobile-based payment initiation is done through the bank branded PL Pay app installed on a mobile device which is integrated with the IC IOS.

Once the mobile P2P payment has been initiated, it follows the clearing and settlement steps which take approximately 10-15 seconds. The Payee bank updates their customer’s bank account balance, and sends a notification to the PL Pay app on the receiving smartphone or PC based PrivateLine PL Pay app. The bank branded PL Pay app for mobile device or PC provides access to the bank PrivateSite to access payment receipt and all other bank PrivateSite functionality offered.

The PL Pay app contains a note field to send contextual data with the payment. There are a variety of uses of the note field, should the user wish to use it. It may reference a purchase, loan, gift, or friendly note of courtesy. The recipient PL Pay app displays the note. The note is encrypted in a manner a bank cannot decrypt for privacy purposes.
PART A, SECTION 3: USE CASE BY EFFECTIVENESS CRITERIA

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

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

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

IMPLEMENTATION TIMELINE

IC IOS IMPLEMENTATION TIMELINE

2 MONTHS: DEFINE REQUIREMENTS WITH FI's
2 MONTHS: MAPPING TO FI CUSTOMER ACCOUNT SYSTEMS
6 MONTHS: COMPREHENSIVE TESTING
2 MONTHS: FI BRANCH EMPLOYEE TRAINING & PROVISIONING
4 MONTHS: FI CUSTOMER PROVISIONING

18 MONTHS TOTAL

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

If the banks adopt simultaneously, it will take 18-30 months for all bank account holders, consumers, and organization to be provisioned and operating. This timeframe includes installation and mapping of the IC IOS TSS banks and credit unions.

This is doable only if a strong regulatory impetus is provided by the Federal Reserve and other banking regulators. The lack of such an impetus will extend the implementation schedule significantly.

Six months have been allowed for usability, alpha, and beta testing of the solution.

Banks should absorb the implementation costs to adopt PL Payments, including server hardware, IC IOS mapping, customer enrollment, and ongoing maintenance for two major reasons:
1. Insured, real-time payments present the biggest new fee opportunity of the century.

2. PL Payments obviates all cybercrime associated with the World Wide Web. Major bank cybersecurity expenditures are simply enormous and are still failing to solve the problem. As an example, JP Morgan Chase will spend $500 million on cybersecurity in 2016, but according to Forbes, “This, however, still has JP Morgan’s legal team wondering if the $500 million is enough.” The cost for JP Chase to implement PrivateLine, just to replace web-based online banking would be a small fraction of that cost. With PrivateLine in place, installing the Trusted Settlement System to enable ICN payments would cost even less. Licensing/maintenance costs are minimal and can be negotiated on a license/item fee or License/maintenance fee or a combination of the two. With ICN software, JP chase would obviate all web-based cybercrime for a lot less than $500 million. JP Chase could also move internal, web-based communications to the ICN, thereby protecting the bank, its officers, employees and their customers.

The Implementation Process includes the following steps:

1. After bank-specific requirements are determined, the Trusted Settlement System (TSS) and IC IOS Control Bridge are mapped to the bank customer account and/or permissions systems at the time of installation.

2. Bank clearing organizations can participate in this process for their banks if owner banks desire, but IC is not dependent upon this scenario. Our integration and mapping experts, working directly with bank IT personnel, can complete the installation of the IC IOS with the Control Bridge as the provisioning and registration software.

3. Community bank software providers can participate in the process as indicated in the previous point.

4. Banks enroll and provision their individual customers via their own operations centers and branches using the IC Control Bridge. The Control Bridge generates identity and authority certificates in the manner described in Addendum A and in the discussion in Section A of this document. Without any other bank steps, the Key Management Infrastructure (KMI) enables of host of other benefits on ICN.

5. Once identity and authority certificates have been established for individual bank customers, the bank sends a CD or USB Key to their customer which contains the bank branded PrivateLine PL Pay app.

6. There are no “secrets” mailed out with the CD or USB key, just the UI to connect them to the bank and the insured-secure end-to-end connection occurs.

7. Once PrivateLine has been installed on any device, all other updates, added features are downloaded via the IC IOS, not the world-wide web.

8. Alternatively, bank branches can install PrivateLine on devices in the branch. The installation is done through a Lightening connector (Apple) or mini USB connector (all other mobile devices. The software placed on the mobile device contains the version for a
PC or business workstation. When the mobile device is connected to a PC or other workstation, the appropriate PrivateLine version is installed for those platforms. 

9. Organizations with ten or more employees who are authorized to use the system provision their employees with identity and authority certificates, which through the Key Management Infrastructure (KMI) are recognized by the ICN Servers at banks. These identity and authority credentials must match the corresponding credentials and permissions in the bank customer account and employee permissions systems.

10. By contract, InterComputer can perform the provisioning, registration and employee maintenance functions for very small firms with limited users.

11. With the aforementioned software installation, banks may want to deliver online banking over PrivateLine verses the current, risky web-based online banking.

12. They can use their existing PHP and HTML coding, but IC has a migration process which removes web URL addresses. All functionality existing in their current web offering can be ported to PrivateLine which also has some browser-like functions for accessing and using a bank online software functionality in the secure ICN environment.
   a. Frustrating short session timeouts are not necessary.
   b. All web cybercrime is obviated.
   c. The IC IOS InterOperating system protects from potential TCP/IP vulnerabilities.
   d. The directory structure is built as each organization and/or individual is added to ICN, with the capability of forming business and personal connections based on the Key Management Infrastructure (KMI) of ICN to maintain person and system integrity.
   e. All nodes on ICN are equal strength.
VALUE PROPOSITION AND COMPETITION

Value Proposition

The ICN delivers the value of trusted digital interoperability to the business and consumer masses. The functionality is unsurpassed because of its foundational technological principles. That value is overwhelming as it brings down the cost of making and processing payments and making funds available for immediate re-use, thereby increasing the velocity of funds and economic activity on a macro scale. Because the ICN is designed for mass use, the costs for its services are less than existing legacy systems. At the same time, the ICN enables banks to replace lost NSF revenue with new revenue sources. InterComputer has already provided a detailed analysis of the revenue available to the top 30 banks in the U.S. These sources of revenue included added value for providing bank branded PrivateLine, real-time payments and other value added services. The total from our analysis $63,522,377,544. The pricing used was very conservative, utilizing close approximations of the overall consumer and business customer base. This revenue number more than compensate banks for lost NSF revenue, which is a punitive form of revenue. InterComputer’s bank revenue analysis document is available upon request.

There are many other bank services currently not possible under the operating risks of web-based delivery mechanisms, which can be done privately, reliably and legally via the ICN. These include lending operations, escrow services, wealth management services etc.

The value to the business and consumer customer is absolute confidence that financial information and transactional activity from Point of Sale to web purchases, to absolute confidentiality of proprietary business activities and pricing etc.

InterComputer seeks to share per item revenue with sending and receiving banks which includes transaction insurance to cover residual risk. The per item amount is relatively small, while banks yield on payments revenue will increase through value-added benefits of immediate funds availability (more transactions sooner) and the considerably reduced costs of using legacy mechanisms both in-house and collectively.

Ally Bank and Goldman Sachs seek to be depository banks in online settings. There will always be a need for bank branches, but the services which can be delivered from banks to bank customers will help reduce the reliance on brick and mortar branches.

The value proposition of the obviation of web cybercrime through use of the PrivateLine PL Pay, the IC IOS, PrivateLine, and tMail for banks to communicate safely with their customers is historically enormous.

The public web will always be there for anything which should be made public or for which no one gets hurt if information is made public. The Private Internet (ICN) will facilitate the use of
high-value information such as real-time payments, financial information, and business transactions.

**Competition**

Competition can be analyzed from several points of view. Banks can compete for customers by setting prices according to new value-added services plus the lower cost of doing business.

Retailers, web or brick and mortar, will benefit from lower payment processing costs, receiving non-credit card payments in real-time, and making it easy for customers to pay “cash” for purchases through their mobile devices. They also benefit from reduced liability and insurance costs associated with theft of financial information and fraudulent charges. Essentially, they can be more profitable, more efficient, and find new ways to compete.

Bank service providers can benefit from the use of the IC IOS. They can re-purpose many applications for their bank customers to use many of the services.

There will be some displacement of organizations in the near to mid-term which are tied to legacy systems, or which seek to provide certain software components which do not enable IC security standards. They can, however, use the InterComputer SDK to adapt existing solutions or create new ones which can add value to banks and bank customers by integrating with the ICN.

**VALUE PROPOSITION AND COMPETITION EFFECTIVENESS CRITERIA ASSESSMENT**

U.3 (Predictability) – The ICN is currently very effective at satisfying criteria U.3.

E.1 (Enable Competition – The ICN is currently very effective at satisfying criteria E.1.

E.2 (Capability to enable value-added services) – The ICN is currently very effective at satisfying criteria E.2.
INTEGRATION EFFORT

B2B Use Case

Points of Integration

1. For a mapped or integrated application, the IC IOS is mapped to the treasury management or accounting system either through an API or in direct coordination with large ERP suppliers such as Oracle and SAP (neither of whom use APIs). Interconnection with these systems require vendor personnel to work with IC personnel to achieve mapping for end-to-end automation, or at least the payment and remittance functions.

2. Standard small business systems such as QuickBooks and Sage products have an API which is already mapped to the IC IOS. When provisioning employees, these systems are shown in the application drop down box for authorizing personnel to use any or all of the end-to-end process.

3. The specific connection points of mapping between systems for end-to-end purchase to payment transactions are related to the data input/output points of each candidate process. For example, when both sides of B2B transactions including the A/R and A/P modules of their accounting software are mapped, remittance data can travel directly across ICN as opposed to traveling with the payment data. The remittance data is encrypted in a way banks cannot decipher. But mapped systems provide full end-to-end data communication efficiency from pre-purchase activity to purchase decisions to payments.

P2B Use Case

Here the power of ICN is demonstrated nicely; connections points are easy to establish. Once individual bank customers and organization customers are provisioned with personal ICN digital identities and authorities, they can interconnect quickly because the Key Management Infrastructure (KMI) of the ICN enables individuals and businesses to quickly established payment relationships. The person’s credentials have been vetted and can be relied upon. Payment transactions can be on a one time or continuing basis.

Once an online payment is made, the corresponding messages are sent out-of-band of the web and reaches the web retailer’s account along with the corresponding payment notification. This feature removes a large threat and constant flow of small and large web related fraudulent payment activity. Hackers cannot intercept the payment information or the payment instruction, neither can they steal financial information from a web connected database.

This may sound simplistic, but we have made complex technology and processes very user friendly.
B2P Use Case

The connection point of this scenario is the reverse situation of the P2B. Businesses paying individuals for any reason, such as refunds, direct purchases, etc. simply establish an interconnection between the parties because they are both on the ICN.

P2P Use Case

The connection point for establishing P2P connectivity is as simple as P2B and B2P. The individuals already have identities and authority certificates issued by their bank. The two parties simply interconnect on the ICN as prompted. One can send payments and notes or contextual data to the other at will, or on a schedule.
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

UBIQUITY

Self-assessed rating:

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

Justification for U.1:

PL Payments enable any entity to initiate/receive payments to/from any entity consistent with applicable legal restrictions. There are no significant technical barriers to adoption; the average consumer, company, bank, or other organization will not find adopting and using PL Payments to be beyond their abilities. PL Payments deliver game-changing value to all parties through a real-time process, insured payment security including the face value, superior operating efficiencies for businesses, and new fee opportunities for banks.

InterComputer’s mobile device technology (not fully defined in this proposal) has hardware/IC IOS capability to store digital cash, referred to as eCash™. Non-bank account holders can have a paycheck or other payment transferred to their device for ordinary use at Point-of-Sale, paying landlords, utilities, grocery stores etc. If a mobile phone is lost, the electronic cash cannot be used by someone else. IC technology both ensures and insures this capability. Upon notification, the remaining cash in the mobile device can be replaced, because a record of the electronic cash account is kept in IC databases. Mobile eCash may motivate non-banked individuals to open bank accounts and use eCash or PL Payments. Over one-half of all payment transactions in the U.S. are made with cash. If one-half of these
transactions can be put in mobile devices, a lot of paper currency can be removed from the system. Over time, people will become more comfortable carrying as much mobile eCash as they want instead of paper bills in physical wallets. When banks cash a paycheck and transfer eCash to mobile devices, they can charge a transaction fee, a much smaller fee than check cashing firms charge. There is more to this issue which can be addressed separately.

**Justification for U.2:**
PL Payments are accessible by all popular fixed and mobile computing platforms on a 24/7/365 basis. Payer and Payee confidential information is securely protected.

**Justification for U.3:**
The features, characteristics, legal rights, costs, dispute resolution procedures etc. are fully communicated to each user and applied rigorously and identically to all users on every transaction. The user experience is nearly identical regardless of which device is used for access. All messages within the ICN use ISO 20022 XML syntax.

**Justification for U.4:**
PL Payments allows for the concomitant, secure, simultaneous transfer of contextual data, in plain text or in popular document/graphic formats, with each payment. The system is already interfaced with the popular QuickBooks and Sage 50 general ledger systems by plug-in, and can be mapped to any enterprise applications for pre- and post-payment business activities.

**Justification for U.5:**
PL Payments can support cross-border payments but has not yet demonstrated that capability. The plan to do so is detailed in the Assumptions section of this document.

**Justification for U.6:**
PL Payments fully supports all of the target use cases defined in Part A, Section 2 of this document.
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>Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.1 Enables competition</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.2 Capability to enable value-added services</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.3 Implementation timeline</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.4 Payment format standards</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.5 Comprehensiveness</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.6 Scalability and adaptability</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.7 Exceptions and investigations process</td>
<td>X</td>
</tr>
</tbody>
</table>

Justification for E.1:

PL Payments offer a level playing field for banks, credit unions, and other FIs to deliver significant added value to their customers. Our solution fosters competition by allowing FIs to brand and price PL Payments without constraints imposed by InterComputer. If a person or organization changes banks, their digital identities and authorities are revoked by their prior bank. The new bank registers their new customer via the Control Bridge and mints new digital certificates accordingly.

Justification for E.2:

The mapping of the IC IOS to FIs customer account systems provides the perfect opportunity for banks to offer value-added services using PL Payment results information. The ICN Software Developer Kit provides gateways for providers and other software developers to create value-added applications that run on the IC IOS and benefit from its inherent security features. For example, digital signatures used for authorized people to sign bank documents are electronically signed using the strong X.509v3 digital certificate according to the pattern...
established in sending a payment, i.e. a two-step acceptance format to create legal irrevocability with digital certificates minted uniquely for that individual.

**Justification for E.3:**
Our credible implementation plan is outlined in Part B of this document.

**Justification for E.4:**
All PL Pay messages utilize the ISO 20022 format and syntax. The ICN is currently very effective at satisfying criteria E.4.1, E.4.3, and E.4.4. The ICN is currently somewhat effective at satisfying criterion E.4.2. The ICN is not now, never has been, and never will be effective at satisfying criterion E.4.5 because doing so is antithetical to the insured-secure nature of the ICN. If something goes wrong with a PL Payment, transaction insurance covers the loss in full. What do you think would happen when something goes wrong with your payment made on a transparent, open source system published by a standards development organization?

**Justification for E.5:**
PL Payments rigorously supports each of the 8 steps in the payment process, as detailed in Part A, Section 1 of this document.

**Justification for E.6:**
The technical design of PL Payments is globally scalable; Lloyd’s certified as much by underwriting the security of PL Payments without geographic restrictions of any kind.

**Justification for E.7:**
PL Payments is designed to be fully auditable and automatically compliant with applicable Federal and state regulations. Multiple layers of patented technologies make this possible.
## SAFETY AND SECURITY

### 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>Safety and Security</td>
<td>S.1</td>
<td>Risk management</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.2</td>
<td>Payer authorization</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.3</td>
<td>Payment finality</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.4</td>
<td>Settlement approach</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.5</td>
<td>Handling disputed payments</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.6</td>
<td>Fraud information sharing</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.7</td>
<td>Security controls</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.8</td>
<td>Resiliency</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.9</td>
<td>End-user data protection</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.10</td>
<td>End-user/provider authentication</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.11</td>
<td>Participation requirements</td>
</tr>
</tbody>
</table>

### Justification for S.1:

The fact that PL Payments are fully underwritten by Lloyd’s against loss due to any kind of cybercrime or system malfunction certifies that all systemic risks have been managed and all residual risks have been eliminated through insurance coverage.
**Justification for S.2:**
PL Payments require explicit, informed, and confirmed Payer consent multiple times during the payment process. Payment preauthorization is both allowed and revocable.

**Justification for S.3:**
PL Payments Legal Framework, applications, processing systems, and transaction insurance combine to deliver real-time payments that are cleared, settled, and legally final in less than 15 seconds.

**Justification for S.4:**
PL Payments Legal Framework, applications, processing systems, and transaction insurance combine to deliver real-time payments that are cleared, settled, and legally final in less than 15 seconds. There is no lag time or risk. Good funds are debited upon payment instruction from sender. At that point the funds are sent to the recipient in 15 seconds with absolute legal finality and immediate funds availability.

**Justification for S.5:**
It should be noted that since all PL Payments are non-repudiable, a request from the Payer for a voluntary refund from the Payee is a simple, plain language message. Such a message can be sent by phone or text or e-mail, or by the ICN’s PrivateLine app. Regardless of the transmission mode, the message is not legally binding on the Payee and will never be seen by the TSS or by either bank involved in the original transaction. If the Payee chooses to “refund” the original payment, he can do so by initiating a new PL Payment of the same amount. Note, however, that the original payment and “refund” payments are not linked in any way within the PL Payment Legal Network. Neither bank, nor InterComputer, has any obligation to act regarding a “refund” of the original, legally final PL Payment. This removes responsibility from the banks for settling disputes between their customers.

**Justification for S.6:**
The ICN is currently very effective at satisfying S.6.1 through S.6.7 because the mere sharing of fraud information via a centralized repository has no effect on real-time payments. ICN’s digital identity/authority certificates, multiple layers of protection (including abuse and potential abuse detection), TSS operations and full value transaction insurance all work together to prevent fraud in real-time. Should a number of incidents become sufficient to indicate a fraud pattern, any user’s digital credentials can be immediately suspended or revoked by the issuer to preclude any further incidents. (S.7.3) Sharing any generalized form of technological fraud information (beyond the identity of the perpetrator) with non-real time systems would have little to no value in preventing future fraudulent actions. The nature of the ICN makes all such information sui generis.
**Justification for S.7:**
The PL Payments solution is currently very effective at satisfying S.7, as witnessed by our U.S. Patent 8,380,622 B2 and our underwritten status by Lloyd’s.

**Justification for S.8:**
The PL Payments solution is currently very effective at satisfying S.8, as witnessed by our U.S. Patent 8,380,622 B2 and our underwritten status by Lloyd’s.

**Justification for S.9:**
The PL Payments solution is currently very effective at satisfying S.9, as witnessed by our U.S. Patent 8,380,622 B2 and our underwritten status by Lloyd’s. Payer and Payee only know each other by an ICN identity, and cannot see each other’s account numbers or any other personally identifiable information.

**Justification for S.10:**
InterComputer possesses two (2) unique, registered OID’s (Object Identifiers) Issued through ANSI and registered through the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization (ISO). OIDs are values used to uniquely identify objects within the X.500 infrastructure, such as in Directory Services and X.509v3 digital certificates. The X.509 Standard requires OIDs in all digital certificates, in order for the certificates to be used correctly and comply with the standard. Since many companies use an OID, these values must be recognizable by others as true globally unique values.

**Justification for S.11:**
The PL Payments Legal Framework clearly defines, and enforces by contract, the roles and responsibilities of providers and users.
**SPEED (FAST)**

*Self-assessed rating:*

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>#</strong></td>
<td><strong>Consideration Name</strong></td>
</tr>
<tr>
<td>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:**

*PL Payments meets or exceeds the shortest time criteria for this step. We wrote the book on (and have the patent for) real-time payments.*

**Justification for F.2:**

*PL Payments meets or exceeds the shortest time criteria for this step. We wrote the book on (and have the patent for) real-time payments.*

**Justification for F.3:**

*PL Payments meets or exceeds the shortest time criteria for this step. We wrote the book on (and have the patent for) real-time payments.*

**Justification for F.4:**

*PL Payments meets or exceeds the shortest time criteria for this step. We wrote the book on (and have the patent for) real-time payments.*

**Justification for F.5:**

*PL Payments meets or exceeds the shortest time criteria for this step. We wrote the book on (and have the patent for) real-time payments.*
**LEGAL FRAMEWORK**

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

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.1</td>
<td>Legal framework</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.2</td>
<td>Payment system rules</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.3</td>
<td>Consumer protections</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.4</td>
<td>Data privacy</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.5</td>
<td>Intellectual property</td>
</tr>
</tbody>
</table>

**Justification for L.1:**
The PL Payments Legal Framework is detailed in Addendum C of this document. Produced by a major New York technology law firm (which is also a member of the Fed’s Faster Payments Task Force), it is comprehensive and legally binding on InterComputer, and on all PL Payments providers and users.

**Justification for L.2:**
The PL Payments Legal Framework is detailed in Addendum C of this document. Produced by a major New York technology law firm (which is also a member of the Fed’s Faster Payments Task Force), it is comprehensive and legally binding on InterComputer, and on all PL Payments providers and users.

**Justification for L.3:**
The PL Payments Legal Framework is detailed in Addendum C of this document. Produced by a major New York technology law firm (which is also a member of the Fed’s Faster Payments Task Force), it is comprehensive and legally binding on InterComputer, and on all PL Payments providers and users.
Payments Task Force), it is comprehensive and legally binding on InterComputer, and on all PL Payments providers and users.

**Justification for L.4:**
The PL Payments Legal Framework is detailed in Addendum C of this document. Produced by a major New York technology law firm (which is also a member of the Fed’s Faster Payments Task Force), it is comprehensive and legally binding on InterComputer, and on all PL Payments providers and users.

**Justification for L.5:**
The PL Payments Legal Framework is detailed in Addendum C of this document. Produced by a major New York technology law firm (which is also a member of the Fed’s Faster Payments Task Force), it is comprehensive and legally binding on InterComputer, and on all PL Payments providers and users.
### 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 nature of the PL Payments solutions obviates the need for participatory rule making by providers and/or users. Allowing such activity could destroy the inherent security of the system and nullify transaction insurance coverage. We are of the opinion that governance should come by way of government regulators, i.e. the Federal Reserve, the FDIC and the OCC. Suggestions or recommendations made by providers/users for system enhancements are always welcome, but subject to review by the regulatory agencies mentioned.

**Justification for G.2:**

The nature of the PL Payments solutions obviates the need for participatory rule making by providers and/or users. Allowing such activity could destroy the inherent security of the system and nullify transaction insurance coverage. We are of the opinion that governance should come by way of government regulators, i.e. the Federal Reserve, the FDIC and the OCC. Suggestions or recommendations made by providers/users for system enhancements are always welcome, but subject to review by the regulatory agencies mentioned.

Rules or standards bodies have never reimbursed anyone for a single payment error or crime. Do banks enjoy reversing fraud charges for debit/credit card fraud, other cybercrime or major hacks? Wouldn’t all of them rather have an insured-secure technology with only a residual risk? If something should go wrong, it too will be residual, for which the insurers and their actuaries have calculated and recognize affordable, low-cost transaction insurance which creates a profit model for their business. **Everyone**, banks and their customers alike, will prefer a full insurance reimbursement for any payment losses due to system error or criminal activity.
ADDENDA

Addendum A .................................................................................................................................................. 59

THE INTERCOMPUTER INTEROPERATING SYSTEM (IC IOS) ................................................................. 59
  Hosted / Distributed Architecture .............................................................................................................. 59
  Digital Identities and Authorities ............................................................................................................. 59
  ANSI/ITU/ISO Object Identifiers (OIDs) Make InterComputer a Registration Authority ................ 60
  The Secure Interface Device (SID) ........................................................................................................ 61
  Installation Process .................................................................................................................................. 62

Addendum B ................................................................................................................................................ 64
  INTERCOMPUTER INTEROPERATING SYSTEM (IC IOS) PATENT CLAIMS ........................................ 64

Addendum C ................................................................................................................................................ 67
  THE INTERCOMPUTER NETWORK LEGAL FRAMEWORK .................................................................... 67

Addendum D ................................................................................................................................................ 68
  CENTRALIZED ARCHITECTURE, NETWORK OPERATIONS, SECURITY AND EFFICIENCY ............... 68

Addendum E ................................................................................................................................................ 70
  DIRECTORY STRUCTURE ......................................................................................................................... 70

Addendum F ................................................................................................................................................ 71
  THE BIG PICTURE OF THE RISK ENVIRONMENT ............................................................................... 71
ADDENDUM A

THE INTERCOMPUTER INTEROPERATING SYSTEM (IC IOS)

The IC IOS is a proprietary, patented, hosted/distributed interoperating system, which utilizes the Internet TCP/IP protocol (but NOT World Wide Web protocols/formats such as http, https, ftls, or standard email) to enable the insured secure exchange of electronic messages while conforming to all applicable regulations, and organizational policies.

InterComputer has developed straightforward applications that utilize the insured security of the IC IOS over a standard Internet connection. InterComputer has also obtained unique, underwritten insurance against any losses due cybersecurity of any type. This Transaction Insurance coverage includes the face value of money.

Hosted / Distributed Architecture

As the root domain host, InterComputer issues a strong cypher digital certificate for each subdomain (client organization) along with digital certificates for persons designated by the subdomain as official points of contact with InterComputer. The private cryptographic keys associated with these digital certificates must be protected under the terms of the license signing agreement.

The subdomain may, in turn, issue organizational and “designated representative” personal certificates for its own subdomains.

Each subdomain may also issue personal digital certificates for its end users through the Control Bridge application. These certificates include both identity and authority attributes. Thus, they guarantee identity while controlling the type and the degree of the messages a given user may send/receive/authorize. For example, a company or bank could use IC IOS digital identities to limit the type and face value of financial transactions its employees may approve or perform.

Regardless of where ICN servers are hosted, the ICN is inherently composed of fully insured “nodes of equal strength”. There is no “weak link” in the ICN chain.

Digital Identities and Authorities

Insured messaging may only be performed by authentic persons; no aliases or other identity compromises are (or can be) allowed anywhere within the IC IOS.

The creation of IC IOS digital identities and authorities (a.k.a. user provisioning) is performed using the Control Bridge application. Usage of the Control Bridge does not require a technical
background; with basic training, Human Resources staff (or the equivalent) can provision users via the Control Bridge application.

The authority attribute of IC IOS digital certificates automatically creates a continuous record of the entire chain of authorization for every message sent via the IC IOS. This record provides a complete and comprehensive audit trail for forensic investigations. (E.7)

“Provisioning” is the process whereby registered system users are enrolled. This process involves the issuance of an enhanced X.509v3 digital certificate, which includes not only electronic identity but also electronic authority limits. These digital certificates also enable the creation of a complete “chain of command” for all transactions for compliance with applicable governmental regulations and company policies, and for forensic accounting purposes. InterComputer’s Control Bridge application enables banks to provision their individual customers and companies to provision their individual employees.

When the issuer of an authority certificate chooses to change the user’s electronic authorities in any way, the issuer may mint a new authority certificate using the Control Bridge. Once minted, this new authority certificate automatically replaces the obsolete authority certificate and is paired with the corresponding identity certificate.

Each ICN identity/authority certificate is absolutely unique. A user may only conduct transactions using the bank accounts authorized by the certificate. Therefore, an employee wishing to use the ICN to conduct transactions using his personal bank accounts may NOT use the identity/authority certificates issued by his employer to do so. Instead, he must obtain separate identity/authority certificates from his personal bank for his personal accounts.

**ANSI/ITU/ISO Object Identifiers (OIDs) Make InterComputer a Registration Authority**

InterComputer possesses two (2) unique, registered OID’s (Object Identifiers) Issued through ANSI has registered them through the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization (ISO).

OIDs are values used to uniquely identify objects within the X.500 infrastructure, such as in Directory Services and X.509v3 digital certificates. The X.509 Standard requires OIDs in all digital certificates, in order for the certificates to be used correctly and comply with the standard. Since many companies use an OID, these values must be recognizable by others as true globally unique values.

The X.509v3 Certificate Mint requires the use of unique OIDs. These uniquely identify the organizations referenced in electronic components of the X.509 certificate. Furthermore, all OIDs embedded into certificates must uniquely identify entities within the ICN KMI Hierarchy.
The use of X.509v3 certificates across the Internet and certificate-aware software requires that we obtain OIDs within the joint-iso-itu-t (2) arc. In the United States, the law also requires that ANSI maintains a record of all OIDs registered within the joint-iso-itu-t (2) arc. Thus, ANSI provides all registration services for the joint-iso-itu-t (2) arc.

The OID provides InterComputer with values to use in our X.509 certificates as well as using them for future software and/or hardware solutions.

The two organizations that manage OIDs at the root level are the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization (ISO). Registration of OIDs through ANSI for American Corporations ensures registration with both organizations and a unique OID.

InterComputer has successfully registered their OIDs which makes InterComputer the Registration Authority (RA) for all OIDs deeper within the tree. For example, if InterComputer successfully acquires a 2.16.840.1.123456 OID, then InterComputer has complete control over all subsequent registration of OIDs within the tree. InterComputer’s registered OID will be used for the InterComputer Corporate Certificate Authority (CA) for user IDs, and that OID can be used by ICs servers and embedded into all user certificates that it creates.

Having these registered OIDs allows InterComputer to properly mint and distribute certificates and to record all the objects and certificates in their system and all related systems. It also gives them the ability to record all the OIDs in their system to the proper registration authority.

The OIDs also record the proper hierarchy throughout the InterComputer IOS system and works with the ICN for additional levels of validation and authentication.

The registered OIDs are another enhancement added to the IC IOS system to provide the required trust and integrity of the system and all data and messaging within the system.

**The Secure Interface Device (SID)**

The SID employs patented hardware and software to guarantee the identity and presence of an IC IOS end user. The SID accomplishes strong, yet simple three-factor authentication without the use of tokens.

The SID currently operates in soft mode on both Android and Apple mobile devices.

We plan to integrate the SID with specific smartphones in “hard” mode. Once done, the SID will apply rigorous three-factor authentication to any user attempting to connect to the IC IOS.
Three-factor user authentication requires a user to satisfactorily present three factors to the IC IOS: something they know, something they have, and something they are. The first item might be a username/password combination. The second is the hard SID/smartphone itself. The third item is a fingerprint sent via the SID/smartphone. As part of the authentication process, the SID/smartphone sends an “out-of-band” verification signal to the InterComputer Network. (An out-of-band signal uses a separate channel from the main message.) This process authenticates not only the user’s identity, but also his personal possession of the SID/smartphone.

**Installation Process**

The IC IOS, the Control Bridge, and the SID, along with all other InterComputer messaging applications, have no natural market boundaries, i.e., no inherent limitations on the type of application. Any organizational need or process for the exchange of high-value electronic messages can benefit from the insured secure environment the IC IOS delivers.

Eighty to ninety percent of any installation involves standardized software that is the same for every application whether military, governmental, or commercial. The other ten to twenty percent of the installation process involves mapping the organization’s designated existing message handling applications to the IC IOS. Registered banks must enable the mapping of InterComputer’s Interoperating System (IC IOS) to their in-house payment processing application(s).

InterComputer has experience in mapping legacy system software to the IC IOS. In all industries, IT environments and applications differ not only by vendor but by age. In many industries that process high volumes of transactions or maintain large data bases, “mainframe” computers still shoulder a significant portion of the workload. One example is the venerable IBM 390 series, which was introduced in 1990.

InterComputer was selected as a First Line Business Partner by the California Department of Motor Vehicles to create a system for the real-time registration of vehicles at the dealership point of sale. This application required the mapping of the CA DMVs operational data bases to the IC IOS. This information resided on IBM System AS390 platforms, which were a quarter century old. The information was stored in antiquated EDL flat file data bases in plain text format, without any relational query capability. InterComputer’s software engineers were able to conclude the mapping process in a period of three weeks.

Thereafter, the DMVExpress application was installed in dealerships and began performing real-time vehicle registration and plating transactions and other DMV information services.
**Trusted Settlement System (TSS)**

TSS performs all clearing, settlement, and reconciliation functions in real-time with full legal finality. (S.3) Two banks may use TSS to clear, settle, and reconcile payments between themselves without involving a third party clearing service. Alternatively, InterComputer Corporation or a third party clearing service may host TSS to provide these services to banks.

As denoted in Addendum B of this proposal document, Patent Claims 1 through 12 apply to this section of the proposal. Specifically, Patent Claims 1 through 4 apply to bank-to-bank clearing, and patent claims 5, 6, 7, 11, and 12 apply to clearing and settlement involving a third party, or if the third party is a financial institution.

TSS operation is governed by the PL Payment Legal Network, which is described in Addendum C of this proposal document.

The PL Payment Legal Network has been approved by insurance underwriters providing Transaction Insurance coverage from end-to-end against any form of cybercrime. (E.5) This coverage includes the value of the money in the transaction. This one-to-many contract authorizes each bank to establish a correspondent bilateral TSS account relationship with every other bank signatory to the TSS agreement. Since all real-time payment activity occurs within the TSS, any bank transacting payments with any other bank has access to all of the information associated with those transactions.

All banks have a choice of hosting their own TSS servers or having a third party do so. Smaller banks and credit unions may choose to have InterComputer host TTS on their behalf. InterComputer may also establish relationships with community bank and credit union software and service providers to perform this function on behalf of their existing bank and credit union customers. TSS operations are technically well within the typical expertise of any depository institution, large or small. (E.1)

Regardless of where the TSS servers are hosted, the ICN is inherently composed of fully insured “nodes of equal strength”. There is no “weak link” in the ICN chain.
ADDENDUM B

INTERCOMPUTER INTEROPERATING SYSTEM (IC IOS) PATENT CLAIMS
U.S. PATENT NO. 8,380,622 B2

1. A method for finalizing an electronic fund transfer that is matched to an invoice for payment to be made from a first party having a first financial account at a first financial institution to a second party having a second financial account at a second financial institution using a transfer network system in communication with the first party, the second party, the first financial institution and the second financial institution, the method comprising:
   a. receiving an invoice authorization document from the first party digitally signed using a first digital certificate issued by and in accordance with a procedure of a certificate authority in communication with the transfer network system;
   b. authenticating the first digital certificate via the certificate authority to confirm that the signer of the invoice authorization document has the authority to assent to payment of the invoice;
   c. storing a copy of the signed digital invoice authorization document in a database associated with the transfer network system;
   d. sending a payment authorization request from the transfer network system to the first party;
   e. receiving the payment authorization request from the first party digitally signed using a second digital certificate issued by and in accordance with the procedure of the certificate authority;
   f. authenticating the second digital certificate via the certificate authority to confirm that the signer of the payment authorization request has the authority to assent to a transfer of funds from the first financial account of the first party at the first financial institution to the second financial account of the second party at the second financial institution;
   g. storing a copy of the signed digital payment authorization request in the database associated with the transfer network system;
   h. sending a copy of the signed digital payment authorization request to the first financial institution;
   i. receiving an electronic payment instruction from the first financial institution;
   j. forwarding the electronic payment instruction to the second financial institution; and
   k. receiving an electronic payment receipt from the second financial institution.
2. The method of claim 1, further comprising authenticating a device communicating with the transfer network system.
3. The method of claim 1, further comprising transmitting an alert if an unauthorized communication is received.
4. The method of claim 1, further comprising transmitting an alert if a communication includes unauthorized modifications.
5. The method of claim 1, further comprising communicating with a third party facilitating the electronic fund transfer.
6. The method of claim 5, wherein the third party facilitating the transaction is a third financial institution.
7. A system for finalizing an electronic fund transfer that is matched to an invoice for payment to be made from a first party having a first financial account at a first financial institution to a second party having a second financial account at a second financial institution using a transfer network system in communication with the first party, the second party, the first financial institution and the second financial institution, the system comprising:
   a. means for receiving an invoice authorization document from the first party digitally signed using a first digital certificate issued by and in accordance with a procedure of a certificate authority in communication with the transfer network system;
   b. means for authenticating the first digital certificate via the certificate authority to confirm the signer of the invoice authorization document has the authority to assent to payment of the invoice;
   c. means for storing a copy of the signed digital invoice authorization document in a database associated with the transfer network system;
   d. means for sending a payment authorization request from the transfer network system to the first party;
   e. means for receiving the payment authorization request from the first party digitally signed using a second digital certificate issued by and in accordance with the procedure of the certificate authority;
   f. means for authenticating the second digital certificate via the certificate authority to confirm the signer of the payment authorization request has the authority to assent to a transfer of funds from the first financial account of the first party at the first financial institution to the second financial account of the second party at the second financial institution;
   g. means for storing a copy of the signed digital payment authorization request in the database associated with the transfer network system;
h. means for sending a copy of the signed digital payment authorization request to the first financial institution;
i. means for receiving an electronic payment instruction from the first financial institution;
j. means for forwarding the electronic payment instruction to the second financial institution;
k. means for receiving an electronic payment receipt from the second financial institution.

8. The system of claim 7, further comprising means for authenticating a device communicating with the system.

9. The system of claim 7, further comprising means for transmitting an alert if an unauthorized communication is received.

10. The system of claim 7, further comprising means for transmitting an alert if a communication includes unauthorized modifications.

11. The system of claim 7, further comprising means for communicating with a third party facilitating the electronic fund transfer.

The system of claim 11, further wherein the third party facilitating the electronic fund transfer is a third financial institution.
ADDENDUM C

THE INTERCOMPUTER NETWORK LEGAL FRAMEWORK

Each bank enrolled in ICN Trusted Settlement (TSS) signs the same enrollment agreement. It is a one-to-many contract that establishes three foundational obligations:

1. Authorization to establish an auditable ICN TSS direct correspondent bank bi-lateral account with every other bank on the system.
2. The bank agrees that every completed PL Payment is legally final, binding and non-rescindable.
3. The bank agrees to bind their customers to the same terms and conditions, i.e., the “legally final” non-rescindable attribute of PL Payments.

These legal terms and conditions are established with every customer ICN enrollment (by contract between the bank and its customer) and reaffirmed twice, with every PL Payment instruction. Every time a customer makes an PL Payment, these terms and conditions will be presented and must be actively acknowledged and accepted twice by the customer prior to payment execution. (Patent Claim 1,7)

This assent is filed in the IC IOS database associated with the Payer.

The payment instruction is then sent from the Payer’s device to their bank to begin the payment process.

If the Payer and Payee have subsequent grievances or issues between themselves concerning a particular payment, most reasonable people will take steps to settle their differences amicably among themselves. If the Payer and Payee cannot settle a payment issue, they have the court system to help them do so. The ICN relieves banks of the legal and management burdens associated with rescinded or repudiated payments.

In 2007, InterComputer obtained a legal opinion from a major law firm regarding the same “legally binding and final” payments with respect to check images and the Check Truncation Act of 2002. They concluded that business check images cleared and settled in real-time between banks can be legally binding as data payments in context of InterComputer’s Bank Customer agreements. At that time, InterComputer did not request a legal opinion on consumer based check images, which would require a separate legal study.

Business check payment images can be cleared and settled in real-time on the ICN.
ADDENDUM D

CENTRALIZED ARCHITECTURE, NETWORK OPERATIONS, SECURITY AND EFFICIENCY

Some have argued that a centralized architecture, where all provisioned organizations, employees and individual consumer interact and transact, places too much overhead burden on CPU’s, internal memory and storage. This argument holds that messages will be congested and slow.

While outlining the “risk-evaluated” methodology for designing and building a secure system from the ground up, IC’s team of experts determined that for two elements of a “complete” secure messaging system, strong enough for a complete insured secure environment are:

1. All messages must be protected by all layers of protection all of the time.
2. That a network is only as strong as its weakest link, therefore all nodes on the network must be equally strong and maintain the right balance of security and usability.

A centralized secure messaging system was required to meet those objectives. Only with this design can all people and organizations function safely, without fear, with no anonymity, and no limit to the applications and uses cases that can be deployed.

In any other type of interconnected system, the same strength and uniform connectivity is not possible. There will be too many “seams”, “holes”, and other vulnerabilities in a system bolted together from multiple technology vendors. The number of fraudulent transactions, spoofing, and cybercrime will increase, particularly in the environment of the World Wide Web. Wherever there is a web connection to a dedicated network, there is a potential on ramp for cybercriminals. It is absolutely essential that all layers of protection operate on all messages all of the time. It is also essential that all people are provisioned or registered with the same high level of credentials including authorities. The centralized system must be as tight as the hull of a large ship. Water must not leak in. Only then are the passengers and crew safe.

The problem thus became how to design a secure message transfer system that would validate and exchange messages fast enough for real-time transactions and be secure enough to eliminate all risk while being ubiquitously accessible.

It seemed obvious that ubiquity meant using TCP/IP protocols, and that security would have to include the application of especially strong X.509v3 digital certificates. The major remaining question was how to create an architecture that would support all of these requirements.
The answer was a hosted/distributed architecture. InterComputer is the top level host and all messages tie back to the IC Registry Authority. But large organizations operate as a distributed host and are provided with an IC Control Bridge including a built-in CA capable of minting their own enhanced X.509 v3 digital and authority certificates. Simplifying the complex, these digital certificates are used in connection with applications enabled in the control bridge. These applications can be mapped or integrated applications, custom built or mass produced software. These applications can also be stand-alone applications.

Large organizations will provide their own server hardware for IC Validation and Application servers, scaled to fit their need. For example, banks can re-purpose existing servers used in online banking to serve these functions, then scale the software and hardware as needed. The core messaging software (the IC IOS) is designed to run as fast as CPU power, available memory and storage space will allow. Predictable by Moore’s Law, over the years since the IC IOS was built, CPU capacity, memory capacity, storage capacity and ubiquitous high speed TCP/IP telecommunications bandwidth are much less expensive than ever before. This trend will continue.

InterComputer can perform all these functions for smaller organizations and individuals who desire it.

The hosted/distributed architecture allows for completely scalable hardware and software growth as system volumes require. Speed and usability are only limited by hardware and bandwidth.
ADDENDUM E

DIRECTORY STRUCTURE

The IC IOS Control Bridge automatically creates the directory structure used in message initiation, validation, and delivery as organizations, employees, and individuals are provisioned and enrolled. The Key Management Infrastructure (KMI) securely manages connections within the ICN, a role that URLs perform highly insecurely on the World Wide Web.

All enrolled organizations and authorized employees can connect as easily as the general public does on the WWW in an app such as LinkedIn. Organizations may set rules concerning connections their employees may make in their work roles on the ICN if they wish.

The full audit trails of all activity are available to those authorized to view them.
ADDENDUM F

THE BIG PICTURE OF THE RISK ENVIRONMENT

While the World Wide Web is the biggest component of the computing risk environment, it certainly is not the only component. Cyber thieves routinely use ubiquitous legacy systems as a means to their criminal ends. Windows, iOS, .NET, Android, etc. are consistently and successfully targeted to find vulnerable points of entry into devices for criminal purposes.

The CBS program “60 Minutes” recently showed a shocking segment on just how easy it is to hack any cell phone. You can read the details at http://www.cbsnews.com/news/60-minutes-hacking-your-phone/.

Microsoft just announced and issued a critically important software fix for a Windows security flaw affecting every computer running any version of Windows from Vista through and including the newest Windows 10. You can read the official announcement at https://technet.microsoft.com/en-us/library/security/MS16-027.

Approximately 85 percent of the desktop/laptop computers in the world run Windows, and the critical vulnerability announced today could affect every one of them if their system software is not updated per the site linked above.

Microsoft’s .NET framework is constantly being attacked and patched. It various languages such as Visual Basic (Studio) are very vulnerable. Look at your Windows Update “history” and you will see continuing security fix updates for .Net. .Net development using the web is far too thin for the safety of money moving in real-time.

The scale of the potential harm these vulnerabilities cause is breathtaking. While Microsoft claims to have spent significantly to enhance its product security, the “design DNA” of Windows is flawed. Brian Valentine, Microsoft’s senior vice-president in charge of Windows development for eight years, famously told a 2002 company-sponsored development conference,

“I’m not proud. We really haven’t done everything we could to protect our customers. Our products just aren’t engineered for security.”

Like the Windows operating system, attempts to make the World Wide Web secure are afterthoughts not envisioned when the system was created. The WWW is UNSAFE for the exchange of funds and high-value information. The very people who created the WWW have said that it was never designed to be secure, and, given the chance to do it all over again, they would take a much different approach.
The world cannot hold its breath waiting for someone to completely reinvent Windows and the Web to make electronic communications safe. That is why InterComputer’s IC IOS and the ICN exist.

Real-time payments can be breached using combinations of:

1. Legacy hardware, firmware and software technology and networks.
2. Mobile technology using either the cell system or web, open email protocols and Wi-Fi.
3. Software code combined from multiple sources without controls and secure methodologies to eliminate the probability of unknown holes and cracks.
   a. Back doors existing in uncontrolled code development.
4. MS DOS, Windows, .Net, Apple OS and mainframe OS’ were built for functionality, not security. Security has been addressed as an afterthought.
5. Security protections such as tokens are a layer of protection, but relatively weak, and completely breach-able through web based man in the middle attacks, screen scrapers, keystroke loggers and other methods.
   a. The patterns of security tokens, whether sent out of band by text, or QRP codes can be monitored and spoofed simultaneously with other tokens.
6. Email has become a universal conveyer of malware. (Trusted electronic mail is badly needed.)

The fundamental problem underlying all of these, and other issues, is that in the rush to sell and enjoy this fabulous functionality, the electronic framework to keep private data secure has been left out at the time of invention. The brilliant people who invented TCP/IP, the web, and many other technologies simply did not have an “awareness” of the need to design and build security into computer software as they invented and developed it. Their only goal at the time was “make it work.”

By 1990, security issues were sufficiently understood to take effective countermeasures. Why were effective countermeasures not taken? They could not be added as an afterthought; they needed to be “cooked into” the Web’s original design architecture. Hence, the damage and costs in Web-based crime are larger today than they have ever been, and are growing fast.

Bank and FI technologists default to the “web” as a technical means of leveraging the Internet. Too often they stick to it because they don’t know any other way, or take time to learn or believe that standardized software exists which was built for TCP/IP Internet communications without using the web or other open protocols like email and file transfer protocol (FTP). Today, when massive breaches occur, bank executives tend to throw more money at “add-on” security products and services, consultants, etc. as a means of addressing the problem. It is a Sisyphean task because they are trying to solve the wrong problem. The Web will NEVER be secure.
But InterComputer’s IC IOS and ICN were designed and purpose built from the ground up to solve the REAL problem of cybercrime: how to place ubiquitous, secure messaging beyond the reach of cybercriminals.
Faster Payments QIAT

PRELIMINARY ASSESSMENT
Proposer: InterComputer Corporation

APPENDIX A: QUESTIONS TO THE PROPOSER
Ubiquity

U.1.1: Is there a way for end users whose bank is not participating to participate?

An end user may not participate through a bank that is not participating, but they may participate in some way as an unbanked user, which is described in a subsequent section of this document. Banked end users can either ask their bank to participate or change to a participating bank. We expect that a non-participating bank, under sufficient encouragement from its customers, will opt in to the system. Most businesses respond to customer requests.

End users can register with ICN on their own if their bank does not participate. They can use tMail and other features and transact with any other user whose bank does participate for payments, but their payment instructions will be converted to ACH for sending or receiving payments.

Motivation by banks to adopt and implement PrivateLine connections to their customers should be high. Providing customers with a fully functional, standardized, non-web connection to their bank is essential to banks serving their customers with the highest level of service. People are tired of risks and cybercrime associated with web-based online banking. Banks should be tired of the high costs of securing web-based solutions and yet is still risk laden. Banks should be motivated to remove web-based access to cybercriminals into their online systems or penetrate their internal systems.

A PrivateLine connection from banks to their customers enable banks to offer many more services which web online banking is not strong enough to support. Examples are establishing new accounts and loan origination documents signed by strong X.509v3 digital certificates unique to each customer. The benefit of a non-web, standardized, Bank branded, insured-secure, PrivateLine connection not only value added services, but critically paves the way for ubiquitous real-time payment with peace of mind.

U.1.1: How are payees set up inside the solution?

Summary:

The bank sets up an end user via the PrivateLine Control Bridge UI of the IC IOS to generate an X.509v3 digital identity certificate and a separate X.509v3 digital authority certificate, which are unique to that end user. The Control Bridge simplifies the creation of both digital certificates, and completes customer provisioning in a single step. Access to the Control Bridge by bank employees is governed by the authorized hierarchy established by the bank at the time of installation and mapping via the AuthoriTree feature. All employee authority certificates are signed by the digital certificates of those in authority in the chain of command. Authorized employees at the Branch level use the Control Bridge to register and provision end users, whether companies or individuals, for all ICN or Bank applications, including PrivateLine Payments. (Note: We do not disclose how private keys are protected for identity and authority certificates upon generation.)

Existing customers are set up based upon their existing account data according to prior vetting and KYC procedures. New customers are provisioned and set-up at the time of account opening.
PrivateLine Control Bridge provisioning provides banks with the opportunity to dynamically establish, 
reconfirm or update their customers’ relevant personal or business information, accounts, and 
authorizations. In addition to the user information, the Control Bridge enables the definition of roles, 
authorities, tasks, mini-roles and mini-tasks. It provides banks with the opportunity to offer their 
customers tremendous flexibility and granularity in defining exactly what customers can or cannot do and 
set appropriate limits. Once set up, all authorities and rules are automatically enforced in every digital 
message.

The bank sends their customer either a CD, inexpensive USB key, or Micro SD card to their home or 
business address via postal mail. The CD or USB Key contains the client side of PrivateLine (it replaces a 
web browser with a standardized PrivateLine UI). There are no secrets or customer information on the 
hard media. The out-of-band hard media enables anyone with a PC/mobile device to get onto PrivateLine 
and then connect to their bank. Once an individual or businesses has one client side connection to ICN, 
they never need hard media again. This is similar to the old CompuServe method, followed by AOL and 
others later on. We do not allow web-based download for the PC Client to ensure a perfectly clean, 
untainted client installation.

Recipients of hard media do not need to go to a bank branch for any set-up or connection purposes.

If bank customers only use mobile devices and these devices do not have USB or Micro SD ports, they 
can go to a bank branch and receive the client side of PrivateLine via Wi-Fi inside the branch.

A detailed explanation of the functionality of the PrivateLine Control Bridge follows. It is presented here, 
in full, only once out of respect for the reader’s time. Answers to other questions may simply refer to this 
section.

PrivateLine Control Bridge

The primary component of the InterComputer IC IOS Application Programming Interface (API) is the 
PrivateLine Control Bridge. It functions as a powerful, comprehensive administration console to authorize 
and provision (register) mapped applications and users to interoperate within the insured secure digital 
trust environment of the ICN. It generates enhanced X.509v3 identity certificates and enhanced X.509v3 
digital authority certificates. It enables users to connect to ICN applications and defines what users can do 
within those applications. In this way, organizations can completely secure and manage their digital 
interactions with their customers.

The PrivateLine Control Bridge fits any desired interconnection or intra-connection requirement between 
or within organizations.

The Control Bridge is standardized software, which intuitively simplifies many complex tasks. The 
standardized nature of the Control Bridge also delivers the ubiquity of access to 21st century trusted 
digital interoperability the Fed has set as a key characteristic of any successful solution. Whether 
messaging inside an organization or crossing organizational boundaries, it eliminates the barriers between 
large and small companies and their end-user employees and customers.

The Control Bridge also contains configurable abuse detection and potential abuse detection capabilities. 
Rules can be defined and added as required by each organization or defined by Financial Services 
Governance Committee. From a functionality standpoint, the term “abuse” includes “fraud”. Potential 
Abuse and Potential Fraud rules invoke the same response to suspicious messages by the system. The 
difference between abuse and potential abuse is that “abuse rules” stop a message and provide an alert to 
the appropriate personnel and/or entire bank user base. Potential Abuse rules highlight potential issues 
which are allowed to pass through the system but are flagged for further study to determine whether the 
message activity is related to abuse or is a harmless anomaly. These two programs provide maximum 
flexibility to organizations’ loss prevention efforts. Since all messages are tied to organizations, 
employees, customers, or individuals, determining if a potential abuse is indeed an abuse is
straightforward. Both Abuse Detection and Potential Abuse detection provide the ultimate in control to any organization to detect and/or stop malicious messages.

The Continuous Audit application is also accessible from the Control Bridge. Any message can be audited from end-to-end by authorized personnel. (Note: For end-to-end payment message audits, the access to review any single payment, group of payments or complete customer payments is accessible within the Trusted Settlement System (TSS).

A company will use the PrivateLine Control Bridge to:

- Provision (register) employees with enhanced X.509v3 digital identity certificates. (The protection of private keys and cross validation exchange of public keys in the messaging process with signed messages is not disclosed.)
- Provision (register) employees with digital authority pertaining to roles, tasks, mini-roles and mini-tasks in an authorized, hierarchal chain of authority and to use mapped, in-house applications or external ICN applications.
- Provision organizational or individual customers (e.g. business partners, service providers, vendors) with specific authorities to connect and interoperate on ICN.
- Provision applications used in house or between entities or any other desired party.

The AuthoriTree™ component of the Control Bridge is visible in an organization chart format but contains the authorities for each subsidiary, division, or department which have been assigned. It enables anyone with the required authority to see all the people within the organization structure who are provisioned to use any part of the system, and displays the authorizations for which users are provisioned.

The degree of granularity used in assigning specific authorities and limits is entirely up to the organization.

For banks, the business customer base is provisioned at set-up with the authority they have. AuthoriTree displays the people who have been provisioned within the customer organization who have authority to access accounts, make payments and perform other banking functions. Banks may choose to allow consumer customers to use a single digital authority for all their accounts or multiple authorities if applicable. All identities and corresponding authorities are always visible to the bank.

**Ease of Set-up, Maintaining and Revoking Digital Identity and Authority Certificates.**

The most difficult part of establishing a PrivateLine connection with new employees, customers or other business partners is setting up the existing user base for the first time.

Organizations determine which employees will take responsibility for governing the provisioning of users. They will enter data about the employee identity and the authorities into the PrivateLine Control Bridge. After this information is entered, the identity and authority digital certificates are generated by a single command. The private keys are protected (kept proprietary) and the public keys become available in the validation system. The Key Management Infrastructure (KMI) provides dynamic versatility and additional functionality to banks and bank customers and can provide additional ongoing revenue opportunities to banks.

The Control Bridge is available at the bank branch level with authority provided to branch employees who set-up and maintain customer accounts. For initial set-up of existing accounts. Branch employees take the customer account data (individual and/or business) and establish identity and authority certificates based on the KYC procedures and existing account rules at the time of initial account establishment. When the data are entered, the identity and authority certificates are generated by a single command. When an employee leaves an organization, the corresponding organizational identities/authorities/limits are immediately revoked. If an employee’s organizational authorities change, the existing digital authority certificate is revoked and replaced with a new certificate that reflects the appropriate authority changes. If new employees of the customer become authorized to use the account,
new identity and authority certificates are generated as previously described. It is a dynamic, simplified and easy to maintain process.

For individual accounts, both the identity and authority certificates are created and used. Banks can configure the Control Bridge individual account provisioning for authorities reflecting the terms of use for the account.

Conversion of an existing bank customer base to PrivateLine can be achieved quickly, branch by branch and up the bank’s hierarchical chain.

When a bank customer closes an account, all identity and authority certificates are revoked upon command. There is no lag-time in the system for the revoked certificates to be so cancelled across the entire system. Likewise when new accounts are set-up, branch personnel complete their KYC responsibilities and the newly provisioned identity and authority certificates are immediately available in the system.

Although the CEOs of the largest banks can have digital authority to view the entire employee base and customer base in the AuthoriTree format, it is not likely they will wish to do so. But the CEO’s team can assure the CEO, the Board, the auditors, and the bank’s regulators that SARBOX rules are in place throughout the organization and are being enforced in real-time through PrivateLine. If the CEO wanted to test any one division or branch, it can be easily done.

U.1.1: Is it possible to send a payment to an unregistered user? If so, how does that payee access the payment?

Real-time payments to unregistered users are neither possible nor permitted in this solution. However, a registered user can send a payment to an unregistered user via conversion to ACH or Fedwire (as applicable) until all banks and credit unions are on the system.

U.1.6: Are there any participation requirements other than being a bank or FI? Can non-bank payment service providers participate in this solution?

It is possible for money transmitters or, potentially, the credit card providers to use the system if business considerations and conditions exist. If it is desirable, the benefit to adding such entities to the real-time ecosystem is that they will be provisioned on ICN, which will keep all network nodes on ICN of equal strength. This possibility is covered by Patent Claims 5 & 11. (Addenda B in the Proposal)

U.1.3: Does the solution support transactions denominated in other currencies, e.g., can the user transact in Euros or rewards points?

The solution does support payments made in currencies other than the USD. This is explained in detail in the “Proposal Assumptions” section on pages 11-12 of the proposal. But to add clarification of functionality, large banks dealing in multiple currencies can send or receive payments in other currencies directly with international banks that also use PrivateLine, in real or delayed time. Reward point programs can be treated as a currency where bank and bank customers have counter relationships at other banks and institutions which disburse or redeem them. The logic to accommodate these programs and relationships is added as the need arises.

U.1.5: Does the ICN’s plan to gain widespread adoption rely on a Federal mandate? If there is not support from the regulators for this solution, what is the expected impact on the implementation timeline?
Dependence on market forces without Fed impetus may result in a longer adoption curve. However, because the Federal Reserve and their member banks require “measurable network nodes of equal strength,” there is no better way than to embrace and support the system. It’s best to do what it required to do it right the first time. When banks treat their customers and shareholders right, everyone wins.

Delivering cost containment and the ultimate in digital security to their customers should be motivation enough for banks to adopt. The IC IOS and Control Bridge are “standard” software installations; 80-90% of any installation is installing and configuring standardized software. There is a component for mapping PrivateLine to the bank customer account system or modifying their existing web delivery system to remove the web URLs and re-direct the messaging to the automatically-generated directory services created by the Control Bridge. Existing HTML and PHP coding is already in place. In this way banks or InterComputer do not have to re-write their code to begin their on-line banking PrivateSite.

Banks are spending vast sums of money attempting to secure completely un-securable, web-based online banking and back-end intrabank/interbank communications. Once PrivateLine is installed at each bank, these web-security costs, fraud and loss costs are eliminated. The 2012 Federal Reserve Payment Study revealed $6B in fraud losses within the banking system. This cost does not include the related expenses of researching breaches, repairing holes, sharing hack information quickly, heuristically attempting to predict attacks, the high risk of loss of customer information (including biometric data), and the unrecoverable losses caused by reputational damage.

U.2.1: Please describe how end users will set up a payment to a payees or several payees?

For regular B2B payments, invoices are entered normally in either manual or automated mode. The payment date and/or time must be included or added. This functionality is part of the field mapping process every IC IOS installation includes. IC applets are deployed as needed during the mapping process. A long string of invoices may share the same date and time. Further, a long string of remittance data (e.g. invoice numbers) can be included in one payment amount. For multiple payees, each payment is sent sequentially and will be a fraction of a second different in timing. There are no batches, and therefore no batch cutoff times. Payments are processed in rapid, sequential mode according to company policy.

A/P personnel will have authority to reach the first “approval” prompt and accept it. If an organization wants more than one person to use that authority on each invoice, that is a configuration option. At the time payments are due to be made, authorized treasury personnel will accept the second approval screen, and an organization may require additional authorizations. Although payments begin to execute after all required approvals, they will have a slightly different time stamp. Each payment is its own end-to-end process. There is no batching or netting or need for such. The organization’s accounting system will reflect the status of payments made as it normally does.

If unexpected manual payments require paying multiple parties at the same time in a business, that may also be done. The acceptance approval prompts are still required.

For B2C or G2C payments, systems will specify the date and/or time they want mass payments made. PrivateLine Payments work the same as B2B. Although the payee list may be long, payments are sent, initiated and completed sequentially but very quickly. Each payment stands on its own as far as tracking, end-to-end audit or any other requirements.

For P2P payments, there may be a reason to pay a few payees at a time. It is configurable, but the user will see a confirmation screen for each payee selected. There is a default limit of three at a time. This limit may be changed, but unless there is a reason to increase it, multiple payees is an option. Like every other use case, each payee is treated separately in the end-to-end payment process.
With each payee entered into a system for payment, the first acceptance screen will have already been approved by the authorized employee at the entry stage, and the second approval prompt is required at the time the manual payment is actually sent.

**U.2.2: How can the payer ensure that the payment is being directed to the correct payee?**

**VALIDATION**

Once Connections are established, remote validation servers cross-validate the identity and authority certificates BETWEEN buyer and seller in any payment use case. The validation server authenticates and validates the identity and authority certificates and enable the transaction to proceed accordingly. Validation is a key process and is proven whenever any transaction is audited from end-to-end.

**B2B**

When someone enrolls as a PrivateLine user, their corresponding employer or bank gathers required identifying personal information and defines the corresponding authorities prior to issuing a unique digital identity/authority certificate. Likewise, for organizations, the bank business customer provides the employee data and authority data for entry into the Control Bridge before certificate generation. (For existing customers, banks will probably have all of the requisite identity and authority information on file.

**INDIVIDUAL**

InterComputer’s PrivateLine UI replaces the word “Contacts” with “Connections.” In the world of human relationships, connections are stronger than contacts. If the bank customer is an individual, the individual sends a connection request to another individual or an entity which the individual wants to pay. This mechanism is familiar to many as it is similar to LinkedIn (although our method pre-dates LinkedIn) “connections” within the system for cross-validations. However, people and organizations define who is searchable and who can receive or make a connection request.

**CONNECTION**

The recipient of the connect request can accept, ignore, or reject the request to connect. Companies and individuals can choose whether or not to allow their name and employees’ names to be searchable, or restrict the search criteria. Each organization class has the ability to configure or limit its searchability on the system. The “request connection” function works both ways. Either the payer or payee can establish the connections based upon the authority defined in their authority certificate. Other than the smallest of organizations, two employees must approve a request to connect, either when receiving or sending connect requests.

**PRIVATELINE UI LEVEL** - The payer uses the PrivateLine drop down box or search function to select the correct intended payee(s). The payer has clear visibility of:

- An individual name or a P2P payment
- An organization name for a C2B or C2G payment
- An organization name (already tied to specific accounts)

**SYSTEM PATH**

Once the payee has been selected or preselected, the internal system path from end-to-end is without error. For residual risk, should a system error occur, and there is a loss, the transaction insurance backs the system to provide loss damage recovery.
U.2.2: Is there an opportunity to substitute different aliases (cell number, email) for the digital certificate?

Email addresses or telephone numbers may be added to the overall individual or company information in the Control Bridge before generating the identity and authority digital certificates. Each identity and authority certificate is unique to an individual, a company or employee within an organization. But there is no need to substitute or rely on these less rigorous identifiers. In fact, relying on them is far less secure than ICN and PrivateLine. There are no aliases used in the system—only real names for individuals and companies just like those used in DDA accounts and credit/debit cards today. The privacy and security make it easy to maintain digital certificates from initial generation through revocation. It’s easy to revoke and re-generate authority certificates when job responsibilities change. The validation system and overall secure messaging maintain privacy and message integrity.

U.3.5: Under which conditions, if any, would ICN introduce a process to formally support end users disputes with end users who have made a payment error?

ICN can offer a “dispute resolution” process if banks require it. Nevertheless, we think banks could profit from forgoing the expenses associated with “unwinding” real-time electronic payments.

U.3.6: Please describe how end users will know that they can make a payment to a business using this Solution? How will this payment option be branded? Is it as PL Pay?

As described above, an end user may use the PrivateLine search function to select the correct intended payee, whether an individual or a corporation. We anticipate that businesses utilizing this solution may find it beneficial to advertise that fact. “PL Pay” is a short name of the actual name of “PrivateLine Payments”. A “PrivateLine” label or icon is for merchant locations and other methods of making real-time payments.

U.4.3: Can the Solution provide an estimated delivery of the various message format standards to support the sharing of contextual data across all the different transaction types supported by the ICN?

Any associated messages, regardless of format type, arrive with no appreciable time difference from the payment message, i.e., in real-time.

Business partners registered on ICN can use InterComputer’s PrivateBusinessDrive™ solution to rapidly exchange large contextual data files independently of the payment.

Should a non-standard format file become necessary contextual data for a payment, it may be attached to the payment message. Mapping to non-standard applications to enable upstream and downstream processing automation is typically a matter of a few weeks’ effort.

Please describe the implementation required for a retailer to desire and employ PL Pay? Would this be a near-field communication (NFC) transaction only, or would other communication options be available at the point-of-sale (POS)? How would the end user initiate a transaction at a retail establishment?

Please see the answer to question E.6.1 below.
Efficiency

E.1.1: If an end user’s name is their identifier/alias for their digital certificate, how can they have multiple providers?

As explained above, when someone enrolls as a PrivateLine user, their corresponding employer or bank gathers their identifying personal information prior to issuing a unique digital identity/authority certificate. The payer uses the PrivateLine search function to select the correct intended payee. From that point, the system literally insures that the payment will not be misrouted or compromised in any way. If any user discontinues their association with a particular bank or employer, the institution immediately revokes their digital certificate. Under this system, there is no inherent limit on how many providers an end user may have at any given time. For example, one user with multiple employers may have a unique digital identity/authority certificate from each employer. A user holding accounts at multiple banks may have a unique digital identity from each bank.

E.1.3: Please describe how the ICN requires providers to disclose costs/fees to customers in advance of the transaction

ICN has a configurable fee field when it is necessary or desirable to display fees in advance.
Fees or fee policies may also be added to the legal language on each acceptance screen.

E.2.3: Does the Solution require providers to disclose that value-added services are optional? If so, how and where does this occur?

Disclosure of value-add fees is the responsibility of the service provider. Banks can offer value added service offers at time of set-up, or any other time agreeable to customer preference. Several methods are available to banks to do so.
Please see the answer to question E.1.3 above.

E.3.1: What are ICN’s credible market share and growth projections? What is the proposed plan to provide integration support for all the banks in the US if the banks are simultaneously implementing the solution in a four-month period as outlined in the first two chevrons (page 40)?

Two years = 25% market share, three years = 50% market share. It is possible to obtain higher market share faster or more much more market share in three years.
IC deploys two-man integration teams to work with bank IT staff to define requirements and schedules. Large banks will have regional operations centers that need to be mapped as required by their IT topology. Bank IT staff can train and provision branch employees without InterComputer’s intervention.
Should The Clearing House be interested or willing, their resources might be leveraged, and may help to accelerate adoption.
For community banks and credit unions, third party service providers like FIS, Fiserv, and Jack Henry could be integration partners. Credit Union third-party providers can participate in adoption.

E.3.1: What indication does the ICN have that the Fed will adopt this strategy and mandate? As the proposal states, it is only doable "with strong regulatory impetus from the Fed Reserve." What is the Solution’s strategy if the Federal Reserve does not provide this impetus? What effect would this have on the implementation timeline?
Our proposal NEVER STATES that “it is only doable with strong regulatory impetus from the Fed”.

IT is obvious that Fed impetus would accelerate the adoption curve. But

E.6.1: Please describe how the remote P2B use cases will be supported, including payment at POS, and what the merchant investment will need to be to support ICN payments. What hardware and software will merchants be required to have/to purchase if they want to accept payment through ICN?

A detailed explanation of the functionality of the PrivateLine Point of Sale payments follows. It is presented here, in full, only once out of respect for the reader’s time. Answers to other questions may simply refer to this section.

PrivateLine Mobile Point-of-Sale Payments – InterComputer’s PoS Technology

Nationwide, mobile payment adoption to date has been disappointing in view of the fact that there are nearly 330 million mobile phones in use in the United States. Mobile phone manufacturers from Apple, Samsung and Google’s payment (Android Pay) have not made significant dents in the PoS market despite many PoS merchants adding NFC capability to their payment terminals. Smartphones could remove the risks of magnetic strip and EMV chip hacking.

InterComputer technology used on smartphones can remove the need for special/expensive hardware at the point of sale. InterComputer rigorously analyzed the end-user experience as part of the design process of our three-factor authentication schema to require only two inputs at the PoS. The first input factor is a biometric factor (i.e. a finger print on most new smartphones or an iris scan on the new Samsung Note 7). The second user input factor is a password. The third input factor occurs simultaneously with the transmission of payment invoice and total amount due at the point of sale. The purchaser can review all items for which they are paying on their smartphone. To accept the total due and complete the payment, the user touches the “acceptance” prompts as provided. It’s literally touch-touch or click-click. (Detailed information of the full three-factor mobile solution is available after signature of a negotiated NDA.)

The absolute need for merchant hardware can be eliminated in most locations due to the high bandwidth and speed of mobile 4G. 4G (Bluetooth and Wi-Fi) is far preferable to NFC’s limited bandwidth and proximity issues. Digitally signed payments are more secure over the PrivateLine channel.

PoS merchants located where cellular signals are weak can, as an alternative, employ a Wi-Fi router device in their check out areas. The Wi-Fi router is provided and secured by IC at nominal cost. Once the merchant receives the router, they merely can plug it into their Internet connection via an RJ45 cable. Access codes are established by InterComputer and automatically connect the merchant signal to the customer smartphone Wi-Fi radio. (Bluetooth adapters, discussed below, are even less expensive.) They are also provided at nominal cost and secured by IC. The merchant 4G signal, Wi-Fi signal or Bluetooth signal connect accurately because of the digital certificates provisioned by the bank (or InterComputer) at the time of set-up (provisioning).

PrivateLine signed payments transmitted on the PrivateLine channel and its layers of protection move with full security and trust between the merchant payment software, the smartphone, and the buyer and merchant banks. PoS merchants may opt to have both the Wi-Fi device and the cellular connection for backup and resiliency. But Wi-Fi routers and/or associated repeaters are far cheaper than merchant card or chip-and-pin/signature and NFC radios while covering larger check-out areas.

For small merchants, the inexpensive Bluetooth 4.0 adapter integrated to most check out register devices provides enough bandwidth for payment messages to be signed with strong digital certificates and the full security of the PrivateLine channel. The Bluetooth option pairs the mobile device to the smartphone automatically “under the hood” over ICN through PrivateLine PoS, and accuracy is provided by validation of digital certificates. Bluetooth radio adapters are easily installed where PC based or network appliance based PoS hardware is used by the merchant. Larger retailers may have USB or RJ45
connectors on their PoS system, which would enable them to use the Bluetooth option if the Wi-Fi option is less desirable for some reason. Both the Wi-Fi and Bluetooth hardware options can also be used for backup to strong 4G mobile connections.

The current method of proximity requirements of mobile phones to expensive, low bandwidth NFC readers can be eliminated unless the merchant desires to use it for Apple Pay, Android Pay and Samsung Pay. However, other payment service providers can gain access to PrivateLine Pay if they are willing to negotiate with InterComputer. Non-NFC payments are a more robust user and merchant convenience as well and enabling contextual data to be exchanged seamlessly at PoS. Smartphone users can disable the NFC radio and save a small amount of precious battery time.

Implementation

As banks provision their business and consumer customers with a PrivateLine connection for all bank accounts, merchant bank customer connections are already established for real-time money to be deposited to their designated bank accounts. The Trusted Settlement System (TSS) must be mapped to the banks customer account system, but that is a single effort per bank. These are the only actions a bank must make to deliver to their merchant customers a non-web, insured-secure online connection and enable them to receive real-time PoS deposits. Banks’ consumer customers do not have to do anything, except install and set-up the bank-branded PrivateLine app on their mobile devices. (It seems likely that after the value of PrivateLine security is fully experienced by the banks, some will choose to abandon fully the cybercrime-infested World Wide Web.)

The difficult task is to integrate the merchant’s PoS software with PrivateLine PoS. For major retailers custom PoS applications are a joint mapping effort similar to the bank mapping process. API-enabled systems can be mapped with a minimum of difficulty. If mid-to-large merchant’s IT personnel communicate well with InterComputer’s integration engineers, mapping to their systems need not be time consuming or difficult. Most large entities have trained personnel who understand the communication and teamwork required to integrate systems. Mapping and testing durations can be brief when IT personnel work with IC engineers to establish the project requirements, schedule and testing.

Smaller merchants will often use standardized PoS for PC’s or network appliances. API’s are often available and there is a certain level of “write once-use many” within a tolerance of 10% for version differences or special considerations. PoS software vendors can also work directly with InterComputer to create the required interfaces for use by their customer base.

Many small establishments may find it cheaper and faster to purchase a software license for one, or more check out points for popular small business PoS software products which are already mapped.

User Experience

PrivateLine payments operates in the background of a smartphone operating system unless the user wants to toggle it on or off. PrivateLine is ready for any payment request within the system. Here are the user/merchant interactions under 4G, Wi-Fi or Bluetooth options.

4G:

- The user arrives at the PoS checkout station or counter.
- The customer provides the merchant with their mobile phone number. (The mobile phone number is tied to the customer’s public key. The customer’s digital certificate is cross-validated with the merchant digital certificate in the ICN system.)
- The user is prompted to authenticate themselves with a biometric fingerprint or iris scan and password. (This procedure sounds cumbersome, but only takes a few seconds. People are used to using reward cards or entering telephone numbers at PoS checkout anyway. The biometric and password completes the authentication process (the third factor is in the background.)
- The merchant and customer are ready to complete the transaction.
The PoS system sends an itemized invoice and total due amount to the PrivateLine Pay application on the smartphone. The customer can take time to review the itemization on their device if they choose, or just accept the amount due. The customer clicks two acceptance prompts and the funds are transferred in real-time. The merchant can offer a paper receipt if they choose. The digital receipt has been signed by the merchant’s digital certificate and is stored in PrivateLine until the user archives or deletes it.

For the Wi-Fi and Bluetooth options, the customer does not need to provide the cell phone number. The ICN-supplied Wi-Fi or Bluetooth radios are capable of identifying the mobile device. All other steps are the identical to the steps outlined immediately above.

Banks have an opportunity to add invoice and payment receipt storage along with budgeting and spending tools to their PrivateLine bank branded app on smartphones and to the PC equivalent. Payment invoice and receipts can be stored for long periods of time by the user if desired.

E.6.2: How can the Solution scale to address increases in the number of TPPs and transaction volumes? What are the projected volumes and how does the ICN plan to handle these volumes, especially at peak times?

InterComputer will increase and maintain the processing power and bandwidth necessary to stay well ahead of demand.

E.7.2: For what time periods will entities operating at TSS be required to retain transaction information?

TSS has no inherent information retention needs beyond those already mandated by the applicable financial regulatory agencies. “Live” retention durations is configurable upon implementation. When “live” data requirements are fulfilled, it is moved to hard media for further archiving or subsequent destruction.

Safety and Security

S.1.1: What is the process that would be followed in the event that legislation was passed that impacted the individual participants in TSS or the network directly?

The Solution is flexible to accommodate changes in the law. InterComputer’s policy is and will remain full compliance with all applicable law, current or future.

S.1.2: What impact would there be on the solution if the Federal Reserve required it to settle in central bank funds?

Settling in central bank funds will require additional 33% more messaging and mapping to Fed accounts. InterComputer’s Patent Claims 6 and 12 (included in Addendum B in the original Proposal) cover this possibility.

S.1.2: In a model where every bank has a correspondent, bilateral TSS account with every other bank, how would ICN manage systemic risk?

- All systems nodes are of equal strength.
- Payments causing even a hint of a problem are halted instantly for review.
- Banks may instantly revoke, suspend, and reinstate the digital certificates of any of its users.
Please refer to the detailed answer to question S.4.1.

S.1.2: How extensive is the insurance arrangement with Lloyds? Are there any settlement-related situations that are exempt from coverage? If so, what are they and how are they handled? What are the specific credit and liquidity risk exposures associated with these?

The following discussion contains details of the insurance arrangements. It is presented here in full and only once, out of respect for the reader’s time. Answers to other questions may simply refer to this section as necessary.

Transaction Insurance

Bankers are keenly aware that the collective volume of money changing hands in the United States every day is some $14 trillion. The idea that InterComputer has end-to-end transaction insurance that includes face value often raises eyebrows because the typical reaction is there is not enough insurance available on the planet to cover the entire U.S. system. This reaction, while understandable, needs to be better informed. This section will explain what this groundbreaking, eComprehensive transaction insurance is, how it works, and why it is a huge value-add at a very low cost.

This discussion merits a review of applicable fundamental principles. The first is that whatever man can build, another man, given sufficient time and resources, can unmake. There is no such thing as perfection, whether it is building something physical or creating groundbreaking software.

One tragic example is the World Trade Center. The twin towers were superb achievements of modern construction, and the tallest buildings in the world for some years. Every structural and service system was designed and built with astonishing foresight. Their intended design life was 100 years; tragically, they stood for only 26 of those years.

The architects in the early 1970s could not envision Boeing 767s loaded with fuel intentionally striking the buildings. How could a building be designed to repel such an attack with minimal loss of life? They could have made the buildings mostly with solid concrete; such a structure may have withstood the impact of the “flying bombs” but would not be economically feasible or even usable as office space. Office buildings must be constructed by optimizing the balance of safety and functionality in a way that justifies the construction costs.

Today, we have more safeguards (layers of protections) in place to prevent a repeat of the 9/11 attacks. Basically most buildings in the United States are built to last a very long time. Fortunately, there have been no repeat attacks of this magnitude, but there is a residual chance that the defenses now in place may not work for various situation-dependent reasons, most of which involve human error and/or malfunctioning technology. This type of risk is called residual risk, meaning something unanticipated could happen to even the very best designed structures and/or systems. Some may be human error, such as the decision to launch the Challenger space shuttle when cold temperatures would cause a critical O-ring to fail and the shuttle to breakup only 73 seconds into the flight. Sometimes, the cause may be “an act of God” such as earthquakes, hurricanes or tornados.

These residual risks are inherent, “potential”, or lingering risks against which man cannot fully guard.

Just like building designs, digital systems must also balance form and function, i.e., how “open” or “closed” the system is. A digital system that truly enables trusted interoperability must strike an effective balance between security (closed) and usability (open).

Using a parallel example for digital security and cybercrime, one can isolate a computer from any local or wide area network, or the Internet. But in today’s interconnected digital world it’s not possible to gain much benefit from doing so. On the other hand, the productivity gains and desirability of computer networking can be made so open that there is no preventing eavesdroppers, cybercriminals, and
government agents from entering systems and stealing valuable information—and money. TCP/IP digital packet transfer, email protocols, and the World Wide Web protocol were designed for openness, not security. When the world adapted the Web as a means of doing important business, a number of “aftermarket” security measures appeared (such as https). Like most afterthoughts, they have not been effective in delivering digital security, and the Web is more dangerously risky now than it has ever been. Instead of putting Band-Aids on this cancer patient, the only way to deliver true digital security is by going to the root cause of the problem. In this case, that cause is the fact that the Web’s “design DNA” prevent it from ever being secure. The Web will continue to be a great place to distribute as much information to as many people as possible, but it will never play a serious role in the future of secure digital interoperability. That will only be accomplished by a system that was purpose-built, from the ground up, to deliver digital security.

For the past four years, insurance companies have been offering extended electronic data policies for individual customers to include some coverage for cybercrime. Nevertheless, the only technology, that literally insures every message traveling from point A to point B, from end-to-end, at every stage, including payment messages for the value of the money, is InterComputer’s PrivateLine.

The InterComputer InterOperating System (IC IOS) or our core TCP/IP-based messaging system. It was designed and built from the very beginning to deliver digital security with unique identity and authority management features all integrated with multiple layers of encryption and software security components. A defined, risk-evaluated methodology and CMM quality requirements were used from the ground up. After each system and subsystem were flow charted, our team of software security, information security and hardware security experts reviewed each flow to ensure the system met all requirements. This was a long and painstaking process. Part of our risk team included people in the insurance and information risk management professions who helped design the first electronic insurance policies in the 1980s.

We approached Lloyds of London and presented the system as a candidate for end-to-end, eComprehensive insurance coverage for our customers, which included both payment messages and the face value of the money. In 2003 and 2004 we demonstrated the movement of money in real-time between banks in a Financial Services Consortium’s (FSTC) UVX project. After a year’s effort, six underwriting syndicates on the Lloyds exchange created a new e-Comprehensive insurance policy dubbed Transaction Insurance for InterComputer and its customers. It protects all organizations, employees, and customers of organizations which have been provisioned or registered to ICN according to established procedures and operation of the PrivateLine Control Bridge and ICN requirements.

Lloyd’s underwriters and their consultants determined the ICN system is fully reliable, but that there is still a residual risk. Therefore, their actuaries determined that a profitable insurance model existed to justify the underwriting.

Limits on Coverage
To place perspective on the movement of money over ICN in any single hour or day, it’s important to understand that each payment message may be traveling between points during 10-20 seconds on the Internet. But each message is secured from point-to-point by PrivateLine with its multiple layers of protection. No World Wide Web or email protocols are used, thus eliminating web-based and email-based cybercrime. The PrivateLine TCP/IP based messages are heavily protecting identities, authorities and message data via the IC IOS. Each payment message is only traveling in the trusted environment for a few seconds, which reduces risk even further.

InterComputer purchases a minimum limit of insurance per basic requirements, but there is a small transaction insurance fee which is a direct cost in InterComputer’s reasonable transaction fee. As the transactions grow, so does the insurance limit. For example, a $100 Million limit on a base policy representing a base revenue is calculated by our insurers. Each financial transaction fee over and above the base increases the insurance limits incrementally. The more transactions, the higher the fee. The
incremental fees have been calculated to enable a flexible increase in the limit. As the network and transaction base grows, both in the U.S. and globally, the insurance limits grow too. If an event should occur per residual risk, it is predicted to be less than the limit, hence the profit model for the insurers. For example, with the public information disclosed regarding the recent cybercrime at the Central Bank of Bangladesh, involving the Federal Reserve Bank of New York, such a hack could not have occurred, even if done by insiders. But if unauthorized people did breach the system in some way, the transaction insurance would have covered the $81M loss.

Clearly, if the PrivateLine system could be breached to a point or exceeding limits or minimal insurance profitability in a single year or over a period of years, insurance rates may rise or possibly be withdrawn. However, this transaction insurance is now available from other insurers in the U.S. and abroad.

The Policy

The policy is broken into two parts, Section One and Section Two.

Section One (1) – First Party Liability

Fraudulent Electronic Transfers and Attacks

The fraudulent input of data directly into:

- the Insured Company’s Information Processing System
- a Customer Communication System
- a Service Provider’s Information Processing System

The fraudulent modification or fraudulent destruction of Information stored or being run within any of the above named systems.

During Electronic Transmission to the Insured Company’s Information Processing System

- by a Service Provider’s Information Processing System
- the fraudulent preparation of fraudulent modification of any Computer Program
- the malicious alteration or destruction of Information while stored within the Insured Company’s Information Processing System or in a Service Provider’s Information Processing System due to Malicious Code being sent or introduced into such system by any Person
- a denial or degradation of service attach on the Insured Company’s Information Processing System or a Service Provider’s Information Processing System.

Section One (2) – Information and Records

By reason of the malicious alteration or malicious destruction of, or attempt to maliciously alter or destroy:

- Information by any person while the information is:
- Stored within the insured company’s information processing system
- Stored with a service provider’s information processing system
- Stored within an electronic record within the offices or premises of the insured company
- Stored within an electronic record in the custody of an employee of the insured company, designated by the insured company to act as its messenger (or a person acting as a messenger or custodian during an emergency arising from the incapacity of such designated messenger), during the period beginning immediately upon receiving of such electronic record by said messenger and ending immediately upon the delivery of such electronic record to the designated recipient or its agent
Information as the result of a malicious code being sent or introduced by any person directly into:

- The insured company’s information processing system, or
- A service provider’s information processing system; or
- Computer programs owned or licensed by the insured company while such computer programs are stored and/or operated within the insured company’s information processing system

By reason of:

- An electronic record being lost, damaged, or destroyed as the direct result of a robbery, burglary, larceny, theft, or malicious act while the electronic record is:

  - Stored within the insured company’s offices or premises located anywhere within the insured company’s control

In the custody of an employee of the insured company, designated by the insured company to act as its messenger (or a person acting as a messenger or custodian during an emergency arising from the incapacity of such designated messenger), during the period beginning immediately upon receiving of such electronic record by said messenger and ending immediately upon the delivery of such electronic record to the designated recipient or its agent

Stored on a laptop computer or remote computer terminal forming part of the insured company’s information processing system, provided always that the insured company and its employees have exercised reasonable care to preserve such laptop computer and/or remote computer terminal from robbery, burglary, larceny, theft, misplacement, unexplainable disappearance or malicious act

Malicious copying, malicious recording, or malicious sending of any information that constitutes a trade secret identified in the application for this policy of the insured company by any person while the information is:

- Stored within the insured company’s information processing system
- Stored within a service provider’s information processing system
- Stored within an electronic record within the offices or premises of the insured company
- Provided the insured has taken reasonable measures to prevent such copying, recording, or sending of such information.

Indemnification for such loss under this section only applies if such trade secret is listed in the application and when underwriters have expressly agreed to the value of the trade secret. Subject to applicable policy limits and retentions, underwriters’ liability in no event shall be more than the value listed in the application, and trade secret value and loss is subject to verification by the firm listed in Item 12 of the Schedule (at the underwriters’ sole discretion and expense).

Provided always that the insured company maintain systems security levels that are equal or superior to those in place at the inception of this policy.

Section One (3) – Extortion

By reason of the insured having received illegal or wrongful threats, either directly or indirectly:

- To damage or destroy information contained solely within the insured company’s information processing system or electronic records;
- To disclose information
- Contained within the insured company’s information processing system or electronic records or
Which has been solely obtained from the insured company’s information processing system or electronic records

By a person who then demands a ransom as a condition of not carrying out such threats.

Provided always that the insured company and its service providers maintain systems security levels that are equal or superior to those in place at the inception of this policy.

Payments of any ransom pursuant to this insurance agreement 3) shall be effected at the direction of the underwriters, loss control service providers, or their representatives. No cover shall be provided under this policy to any payments as ransom that do not comply with this requirement.

The insured company shall use its best efforts at all times to ensure that knowledge regarding the existence of the extortion coverage afforded by this policy is restricted as far as possible.

Section One (4) – Loss Control Services and Calculation of Business Interruption Loss and Extra Expense

By reason of fees and expenses incurred by the named insured for the services of loss control service provider, solely for the provision of loss control services following the discovery of a loss covered hereunder, but always subject to the sub-limit included in the Schedule, such sub-limit to be part of and not in addition to the Section One Single Loss Limit as stated in Item 8 of the Schedule. The services of loss control service provider shall only be engaged in the event that the loss is likely to be covered by this policy and is reasonably to exceed the Single Loss Retention as stated in Item 9 of the Schedule and then only if the named insured is unable to prevent the effects of the loss by its own diligent means.

By reason of the fees and expenses incurred by the named insured for the services of Ernst & Young in the calculation of Business Interruption Loss and Extra Expense as covered by Insuring Agreement 5 are covered hereunder, but always subject to the sub-limit included in the Schedule, such sub-limit part of and not in addition to the Section One Single Loss Limit as stated in Item 8 of the Schedule.

Section One (5) – Business Interruption Loss and Extra Expense

By reason of business interruption loss resulting directly from a Covered Cause of Loss.

By reason of Extra Expense resulting directly from a Covered Cause of Loss.

Section Two (6) – Information Processing Systems Third Party Liability

To pay on behalf of the Insured damages and claims expenses that the Insured shall become legally liable to pay:

- Libel, defamation, disparagement, or slander
- Invasion of privacy or of breach of confidentiality
- Infringement of copyright, title, trademark, trade dress, or trade name

Plagiarism

An act, error, or omission which causes:

- Prevention of authorized access which is granted to a person other than the insured to the insured company’s information processing system
- Electronic transmission of information to a computer not operated by the insured which causes damage to or destruction of information contained in the computer not operated by the insured
- Breach of system security, including theft of information

Section Two (7) – Rehabilitation Expenses (Applicable to Sections One and Two)
To indemnify the named insured for public relations expenses incurred by the named insured to re-establish the reputation of the insured company as a result of losses covered by either Section One or Two of the policy subsequent to financial loss or losses or to claim(s) being made which are covered by this policy.

(Various provisions)

Exclusions

The exclusions in the policy pertain to the same events which might be perpetrated outside of our system. In other words, the policy pertains to “electronic” data and information contained within the greater ICN system.

S.1.2: What if the ICN’s insurance plan is not available in the market at reasonable prices in the future (what are the arrangements for its renewal and at what terms)? How will the cost of the insurance be covered in future years when the Solution is running at scale?

Industry experience with electronic data policies since 1985 to date has seen only a strong increase in such underwriting activity. Significant volume increases should drive costs down for insurers. Certainly, these policies could have been terminated, but have not. We expect the same with InterComputer’s e-Comprehensive coverage.

S.1.3: Are participating banks required to meet SLAs for network availability? What are the minimum/maximum requirements in these SLAs? Are there any penalties for missing availability targets?

InterComputer is committed to a 99.9% availability via offsite/hotsite mirrored capability. We will require the same of banks that participate in the ICN and we can provide offsite/hotsite mirrored services to those who prefer it.

S.2.2: Please confirm whether the ICN supports pre-authorized payments. If so, please describe in detail how to pre-authorize a payment, including the payer’s ability to initiate, then change transaction parameters?

ICN supports “pre-authorized push” payments, but no “pull” payments of any kind. The payer maintains full control over (i.e. reschedule or revoke) the pre-authorized push payment until the moment it is actually sent.

S.2.2: Can a pre-authorized payment be revoked? If so, how and when? When is it irrevocable?

Payments are not revocable once executed. The word, “revocable”, has no meaning within this solution. The only exception is when the bank has a dispute resolution process in place with InterComputer, in which case the process rules would apply.

S.3.3: Will ICN develop a dispute resolution process if participating banks require it? If not, what would the Solution offer instead?

ICN can offer a “dispute resolution” process if banks require it. Nevertheless, we think banks could profit from forgoing the expenses associated with “unwinding” real-time electronic payments.
S.3.3.: How would the TSS or ICN monitor and enforce the disputed payments process so that end users have a consistent experience across participants FIs?

There is nothing InterComputer can do unless the payer’s and payee’s respective banks are signatories to the same dispute resolution process. InterComputer can offer a standard model for the process if the banks request it. InterComputer’s role in such a process would be defined by its terms.

S.4.1: The ICN describes in detail how it transmits clearing messages and the rules that govern funds’ irrevocability and timing. Please describe in equal detail how funds are settled between the payer FI and Payee FI within the TSS.

A detailed explanation of the functionality of the Trusted Settlement System (TSS) follows. It is presented here, in full, only once out of respect for the reader’s time. Answers to other questions may simply refer to this section.

trusted Settlement System (TSS)

The payment clearing and settlement process and the actual movement of funds occur together in the Trusted Settlement System as defined on pages 24-27 of the proposal. The ledger on page 26 defines the debit/credit clearing and settling process at each phase of the money movement between banks in commercial funds.

To understand the movement of funds for settlement, it is important to note that every payment initiated by any bank customer first must pass a feasibility test (step 1 in the ledger on page 26), which queries the DDA account to ensure sufficient funds to make the payment. If the funds are sufficient to make the payment, the payment process continues to completion. If the funds are not sufficient, the payment cannot begin to go forward and the payer is so notified.

The process for clearing, settlement and movement of funds is:

If funds are sufficient to make the payment, the money is debited from the customer DDA account at that moment.

The bank correspondent account is not like a traditional correspondent account; it is better labeled as a Correspondent Bank Settlement Account or simply a TSS settlement account.

The debit from the customer DDA account is the money, which is set aside to move along the clearing path to the payee’s bank account after all debits and credits have been applied perfectly in the TSS system.

If there is any problem with the messaging concerning debit and credit conditions, e.g. if an imbalance should appear at any time, the money stops with the messages and entries and reverts back to the customer DDA at the payer bank.

Should a message or acknowledgement fail, or if a debit/credit imbalance is flagged and sent as an alert to authorized bank personnel for review.

In this event, the original message is sent through an alternative microburst tunnel. If this second attempt fails for any reason, the money reverts immediately back to the payer’s DDA account and the situation is flagged for further review.

Please follow the flow on the ledger on page 26 of the proposal. There are 12 steps of debits and credits which must be equal in both the send messages and acknowledgement messages.

The “Yes” column in the ledger on page 26 represents that the send and acknowledgement messages have succeeded, and that the debits and credits represented in the “Amount” remained the same from end-to-end.
Continuous Message Audit is active throughout the system and ensures that the messages and acknowledgments have not been altered in any way. If any message alteration is detected, the payments stop and alerts are sent.

Once all messaging is complete, the money has moved and the payment is legally and finally settled. There are no compensating balances as in traditional correspondent bank relationships to keep on account at correspondent banks.

Although the debits and credits are flowing through the system at any given point in time, if payments ceased and all active messages completed, the overall balance in the TSS accounts is always zero. Debits and credits always cancel each other out.

We recognize that there are other accounting entries involved with customer deposits and disbursements on the backend of the bank accounting systems. During the requirement gathering process to integrate to the customer account system, these accounting entries are evaluated and the mapping procedures modified to fit the requirements of each bank.

### Clearing and Settlement with Federal Reserve Funds Option

Our patent claims per the proposal include settlement through third party financial institutions such as the Federal Reserve. If, for any reason, the banks and the Fed determine that payments should be settled in Federal Reserve Funds, it will be necessary to map the TSS system to bank’s Federal Reserve account.

The impact of this method is that a set of payment request and acknowledgement messages are sent to bank’s Fed account and a set of payment messages and acknowledgments from the bank’s Fed account back to the bank for posting to the bank’s customer account.

This method adds one-third more messages in the end-to-end process and approximately five additional seconds to the overall average payment speed at the current time. But the TSS design accommodates this option with ease. Certainly, additional mapping is required.

### TSS Availability to Third-party Non-Bank Providers

Our patent claims cited in the proposal accommodate the potential of third-party, non-bank providers (e.g. qualified money transmitters and even credit companies) should the business case warrant it. It’s important that the business conditions remain neutral or advantageous to our bank customer. The approximately 8,000 banks and 3,000 credit unions in the Unites States are our first priority.

In many cases, banks may benefit from the inclusion of large, third-party, non-bank providers as they all must have bank accounts too. If anti-trust requirements of legislation should mandate inclusion, the TSS system is designed to be inclusive.

From a process standpoint, adding non-bank providers is similar to moving payments through the Federal Reserve. The third party non-bank provider must be provisioned and set-up on ICN. Mapping requirements must be defined and of course, it also adds a third set of messages and acknowledgments. It will add about five seconds to payment completion time.

**S.4: How do you propose that FIs manage settlement accounts across potentially thousands of FIs?**

Each FI has only one TSS settlement account, which is established at contract signing.

Each FI has full view of any payment to which they are a processor/party at all times throughout the entire ICN network.

With 8,000 banks and 3,000 credit unions in the nation, and the current state of IT capability, processing the Fed’s 2012 estimate of 4.5 million hourly ACH/check image payments is a very finite proposition. (It averages about 400 transactions per hour per FI.)
S.4: What visibility will be provided to FIs to monitor and manage these account balances?

The mapping of each FI’s internal account management systems to the ICN provides all required visibility. We assume this question pertains to “account activity” as there are no compensating balances required in TSS. Visibility with any payment, end-to-end with any other bank involved in the payment transaction is complete.

S.4: As the number of FI participants increases, settlement accounts will need to be funded in near real time to ensure end users can transact.

There is no funding required for TSS settlement accounts, ever. The TSS settlement accounts are designed to always have a zero balance when not executing a transaction.

S.4: What funding options are available to FIs?

N/A

S.4: What collateral options are available to FIs?

N/A

S.4: What happens if an FI in the system fails?

The Fed monitors FIs equity and liquidity levels continually. InterComputer will comply with any Fed directives to revoke any FI’s access to the ICN/TSS system. Upon notice of failure, InterComputer will immediately revoke the bank’s identity/authority certificates, thereby preventing the bank from conducting any further operations on the system.

S.4.1: Have you confirmed that transaction insurance be sufficient to satisfy FI risk departments?

Please see the detailed answer to S.1.2 concerning Transaction Insurance. Inasmuch as no other entity can provide this coverage, any FI risk department and/or regulatory body should be pleased to mitigate the overall bank risk profile.

S.5.1: Even with being the type of system it is, the ICN needs to develop rules for handling payment disputes. These rules need to include requirements and SLAs for the participating FIs and clear processes that will support payment disputes due to fraud and end user errors, as well as mechanisms to hold violators accountable. What is the ICN’s intended approach to doing this?

InterComputer’s SLA does contain security policies and rules which are FI’s are already familiar with plus those pertaining to real-time payments. The SLA had to be reviewed by insurance underwriters for approval. These are available for review under NDA.

Many bankers in the past have cited heavy costs associated with dispute resolution. However, if banks wish to provide defined levels of dispute resolution service, the SLA can be modified to accommodate the need. It is suggested that if banks desire or need these rules a Financial Services Industry or TSS group or committee is desirable.
S.6.3: Would the ICN consider the creation and/or management of a centralized fraud monitoring capability that monitors transactions and end user data in the TSS and is shared (as appropriate and if needed) to identify potential trends? This might even be handled by a third party.

The system already contains a centralized abuse/fraud rules and monitoring capability system wide. In effect, the system provides abuse/fraud information sharing in real-time. Rules can be added to the system as they become defined. The same rules operating on all payments are available at the same time.

S.7.1: What rules or requirements would ICN impose rules on providers to better secure the enrollment process with providers and end users?

Please see the detailed answer to question U.1.1 (PrivateLine Control Bridge)

S.7.2: What operational and procedural controls are outlined in the Legal Framework? Are additional ones needed? How will the Solution monitor and enforce compliance with these controls?

We will share the details of the full Legal Framework upon signature of a suitable NDA.

S.7.3: How will the Solution address differences in implementation at individual FIs as they adapt their internal processes, architectures, etc. to accommodate the ICN’s requirements?

The differences among customer account systems are handled by the mapping process at setup.

S.8.1: What are the target availability metrics for the ICN/TSS? For each participating FI? What will the SLA be for a FI to get back up and running if an issue occurs?

InterComputer is committed to a 99.9% availability via offsite/hotsite mirrored capability. We will require the same of banks that participate in the ICN and we can provide offsite/hotsite mirrored services to those who prefer it.

InterComputer has defined incident response procedures (required by our underwriters).

S.8.2: Does ICN/TSS (and/or Lloyds) have business continuity plans and disaster recovery plans in place to support an outage/cyber-attack? Does the system require participating FIs to prepare their own business continuity and disaster recovery plans for their network nodes?

Yes, we have business continuity and disaster recovery plans (required by our underwriting, which includes business interruption coverage). They include complete, hot-site, off-site mirrors.

Participating FIs are required to have their own business continuity and disaster recovery plans for their network nodes and comply with SLA security policies.

S.8.5: When modifications are introduced to the network, is there an end-to-end testing process to validate the implementation? Is regular testing of the entire network contemplated? If yes, what is the proposed schedule and who would conduct it?

All modifications to the network are subjected to rigorous testing, and the network itself is routinely tested (required by our underwriting). InterComputer staff are responsible for the successful performance of all testing activities.
S.9.1: What requirements are in the Legal framework around data protection? Do they require operators and providers to have controls and mechanisms throughout the end-to-end process?

Yes. Most of the security policies banks are already implementing. ICN requires operators to comply with requirements for protecting data as detailed in the SLA.

S.9.3: Can one individual have multiple accounts at the same FI or at different FIs within the Solution?

There is no inherent limit on how many providers an end user may have at any given time. For example, one user with multiple employers may have a unique digital identity from each employer. A user holding accounts at multiple banks may have a unique digital identity from each bank.

S.9.3: Can end users or FIs choose to use other items as aliases (e.g., cell number, email address)? If so, how would this be done and where would this information be stored? As part of the ICN solution centrally, or mapped at each individual FI? How would the TSS account for these differences?

We do not see aliases as being beneficial, but it is possible, and if done the information would be stored on the ICN. Such aliases would only be used as a search or lookup option.

S.10.3: How does the ICN align with all US regulatory guidelines and deliver against this alignment? Please demonstrate.

We fully automate full compliance with Reg E, BSA, GLB, SARBOX, HIPAA, SARS reporting etc. Even KYCC is possible upon presentation of legal documents. For example, the PrivateLine Control Bridge provisioning feature is the ultimate in automatic compliance with all SARBOX requirements, including not only the initiator of a message, but also who authorized it, all the way up the chain of command.

Other examples include automation of SARS and BSA requirements reducing the number of humans required to meet regulatory compliance, and the encryption of payment remittance data traveling with a health insurance or other payments which banks cannot decrypt.

S.10.4: Does the Solution impose minimal security levels for authentication at end user and FI enrollment? What are these and what is the authentication process for both groups?

Please see the detailed answer to question U.1.1 (PrivateLine Control Bridge)

S.11.1: Please share the complete details of the participation requirements in the enrollment agreement with TSS/ICN so the Task Force will understand these for the FI participants (above and beyond Addendum C)

Initially a Registration Agreement (paper document) signed by the appropriate FI Executive begins the process. The FI nominates IT and business officer(s) who will be the point(s) of contact with the bank. The agreement authorizes InterComputer to register the bank and establish a bank identity certificate that is signed by InterComputer’s Registration Authority (RA). InterComputer then provisions the bank as a Certificate Authority (CA) and digital identity and authority certificates are generated and signed for the defined points of contact. Ultimately, bank employees and customers are provisioned in a simplified and easy process as described in question U.1.1 (PrivateLine Control Bridge).

We will share the details upon signature of an NDA.
S.11.3: What monitoring processes does ICN employ to ensure FI compliance with its participation requirements and how does it enforce these requirements?

- A security review is required at the time of setup.
- An annual security audit is also required.
- TSS system is constantly monitored for overall system compliance and around the clock staff attention by InterComputer.
- All messages are automatically subjected to ICN and user company policies at all times.

**Speed (Fast)**

F.4: Please see questions for S.4

F.4: Please provide additional details to describe a settlement option that involves the Federal Reserve, and share how this option addresses the questions raised in S.4.

Please see answer to S.1.2. Configuration and speed are indicated.

**Legal**

L.1.1: Please describe the legal and regulatory obligations that will govern the operation of the ICN, and/or that will impose any compliance obligations on InterComputer or participating FIs? How will participant compliance be monitored and enforced?

Compliance and enforcement with the following compliance regulations are automated and automatically enforced in every message. Although subject to human control, the manpower required to provide compliance is greatly reduced while accuracy and certainty increase.

- BSA
- OFAC
- SARBOX
- GLB
- Federal Reserve Regulation E

L.1.3: How will entities and payments through the payment system (from payer to payee) be legally bound within the proposed legal framework that “governs the operation of the Solution and imposes any compliance obligations on the Solution or end users, and describes any contemplated changes or additions to existing laws necessary to support the solution (L.1.3)”?

The Service Level Agreement (SLA) contains the terms and conditions of use, requirements for use, and the legal language to create absolutely, legally binding finality between banks and their customers who register for the solution. To be consistent, repeatable and reliable, the agreement and its provisions apply to all participating financial institutions. Just as PrivateLine and ICN constitute network nodes of equal strength, the legal agreements constitute a legal network where each participant has the same obligations, terms and conditions.

The first SLA is paper-based and signed at the time of bank set-up and provisioning. Any subsequent changes to the SLA will then be digitally pushed out to all financial institutions at the same time, requiring the digital signatures(s) of the authorized bank personnel to confirm receipt.

Please see below the discussion of an industry committee or small organization who will govern or facilitate required changes.
L.2.1: Please describe the key features of the Payment System Rules that “govern the rights and obligations of all end users, providers, payers, and payees to enable the payment system to operate effectively and efficiently, including the payment system rules addressing L.2.1.1 to L.2.1.9)” (L.2.1). These are not articulated in Addendum C. Please also disclose how the TSS/ICN (or others) will ensure end users’, providers’, payers’ and payees’ continued compliance with all key features?

The banks must modify their customer licensing terms and conditions to include the rules defined in the InterComputer SLA. This binds their customers to the legal framework.

L.2.2: Please describe how the Payment System Rules (please refer to the question for L.2.1) will be developed and amended (and by whom), and how input will be gathered from ICN/TSS stakeholders?

Representatives from financial institutions can be appointed to a committee, or permanent small governance and rules group, established to address ongoing issues related to governance, abuse and potential abuse rules, regulatory concerns, additional customer service needs, functionality issues and improvements. When conclusions are reached, the software and SLA’s are updated and made available to all financial institutions simultaneously.

L.2.5: Please disclose how the ICN/TSS/Payments Legal Framework (or whomever is responsible) will ensure continued compliance with all the key features of the Payment Systems Rules as described in sub-criteria L.2.1?

InterComputer will revise the SLA as conditions warrant.

After initial installation, the SLA is a part of the administrative option of the PrivateLine UI for the appropriate legal employees. Designated authorized employees can review the changes and digitally sign the agreement in this way.

The annual security review has a section pertaining to the SLA and compliance with rules as defined.

L.3.3: Please describe how ICN/TSS/PLF (or whomever is responsible) will develop consumer protection requirements for the ICN if the Federal Reserve requests that they do so?

The Bank TSS Committee will provide input or feedback for implementation of the regulation. The TSS will be supplemented or modified to deliver the additional consumer protection requirements imposed. Bank SLAs will be revised and electronically distributed to participating banks and credit unions.

L.4.1: What are ICN’s/TSS’s requirements regarding data privacy and confidentiality of payment and related data (i.e., contextual data)? Please describe limitations on end users’ and providers’ collection of data and the use or disclosure of payment data to third parties.

All payer or payee payment data is accessible only to the payer or payee and their respective banks. Contextual data is only accessible by the payer and payee, unless there is contextual data directly related to the bank transaction. Otherwise, there is no data collection within ICN or participants on ICN.

If a third-party needs access to contextual data, the payer or payee can use tMail or Contextual Chat. This procedure is at the discretion of the payer or payee. If a government agency or jurisdiction requires contextual or payment data from InterComputer it must be done by duly authorized legal documents.
L.4.4: What are the ICN’s/TSS’s policies around end-user visibility into the data that is collected on them, their ability to limit the sharing of that data, and to change their privacy preferences with regard to the proposed uses of the end-user data collected on them?

PrivateLine and the TSS do not permit data collection. Banks can audit, view or review any payment transaction from end-to-end with the counter-bank to the transaction, including their own customer. But data collection on personal or organizational transactions is not allowed for today’s typical data collection activities.

If for some reason, banks and their customers desire to engage in data collection activities special authorities can be provided in authority certificates. Bank customers must consent through a signed digital document describing the terms and conditions of such data collection. If the functionality is added, end-users must be able to access the data collected and where it was sent.

L.4.5: What is the system’s approach to data breaches (at the ICN, TSS, or a FI/end user level)? Who is responsible for them (including notifications) – this should mention end users and providers if relevant. Does the legal framework (whatever its particular name is) allocate financial or other responsibility among end users or providers if a data breach occurs?

If a system failure occurs, IC is automatically alerted to the problem, and location if applicable.

If there is an attempted breach, continuous system audit and micro-burst tunneling features are activated. The digital message is stopped and re-routed. Alerts are sent to all parties.

If a bank or bank customer determines through the Potential Abuse system that authorized people are engaging in unauthorized activities, that is a “fidelity” issue for the company or bank to address.

If a bank or bank customer determines that unauthorized people trying to engage in unauthorized activity, and the related abuse rules are not in place, the bank and/or bank customer contacts InterComputer and the Incident Response procedures are followed. The contact can come from tMail, tChat, or telephone.

Incident Response procedures provide the method of recording, investigating and correcting any incident not automatically corrected.

Governance

G.1: Does ICN have an alternative governance proposal in the event that the Federal Reserve, FDIC, and the OCC are not willing to take responsibility for governance? Please describe the key attributes of this governance model?

Discussions with various regulators have signaled an acknowledgement of WWW online risks as it pertains to the bank risk profile and now have cyber units devoted to it. An additional interest has been shown in an insured-secure bank connection to their customers that eliminates that WWW online risk from bank risk profiles. They have also shown an interest in insured-secure, real-time payments. We expect regulators have interest in understanding ICN and PrivateLine and may highlight areas they may want to have addressed.

For the alternative governance proposal, please refer to the response to G.2 below.

G.2: Does ICN have an alternative inclusive governance proposal in the event that the Federal Reserve, FDIC, and the OCC are not willing to take responsibility for governance and wish the ICN to bring in input and representation from diverse stakeholders as well as support the public interest? Please describe the key attributes of this inclusive governance model, if possible.
Whether or not regulators want a governance role in ICN and PrivateLine, InterComputer will ask FIs and industry participants to form an independent governance group. This group may be referred to as the Financial Services Real-time Payments Board or something simpler such FI TSS Group. It is desirable to have a diverse group of bank representatives such as Payments Executives and IT Officers as part of the group, representing large and regional banks as well as community banks and credit unions.

The primary purpose of the group will be to meet to discuss issues which may arise pertaining to rules or functionality needed at the bank level and the end-user level. Such a group may propose modifications to the SLA and associated functionality such as:

1. Situations which may necessitate changes to the rules in the SLA.
2. Situations where system functionality needs to be modified or added.
4. Provide recommendations for improving the end-user customer experience.
5. Discuss any other pertinent system issues and notify InterComputer (and if necessary, our insurance underwriters).
6. Discuss any other issues of interest.

Transaction Fees and Value

Bank costs are comprised of one of three possibilities:

1. License and annual maintenance.
2. License and transaction fee combination.
3. Installation and larger transaction fee.

Installation is a one-time expense. License and transactions fee combination is a defined license based on employee customer base and a reasonable transaction fee which includes the insurance. We do not wish to disclose comprehensive pricing in this document, but a typical InterComputer cost for a transaction under $25,000 would be in a range of $.12 to $.22 cents each. We think this cost structure enables FI’s to generate profitable payments revenue. A small fee for large contextual data files may apply.

We have analyzed and produced a real-time payment fee schedule for mobile point-of-sale transactions paid by the merchant in lieu of credit/debit card fees. These fees are smaller than credit/debit fees merchants are used to. Yet, they represent a considerable amount of revenue to banks while lowering the cost of transacting purchases.

The solution offers new sources of revenue to the banks. A document identifying new revenue opportunities and a detailed fee matrix is available upon request.
Section S.1 – RISK MANAGEMENT

OUR Rating: Very Effective

QIAT Rating: Somewhat Effective

Section S.1.1 – Unexpected Legislation

CRITERIA: “S.1.1 Address the risk of an unexpected application of a law or regulation.”

QIAT Question: “S.1.1: What is the process that would be followed in the event that legislation was passed that impacted the individual participants in TSS or the network directly?

OUR Answer: The Solution is flexible to accommodate changes in the law. InterComputer’s policy is and will remain full compliance with all applicable law, current or future.”

JUSTIFICATION: It is impossible to answer a vague, hypothetical question such as this in detail. Other than legislation that would shut down the system, flexibility is the only option.

Section S.1.2 – Settlement Approach

CRITERIA: S.1.2 Address risks related to the Solution’s Settlement approach (see S.4).

QIAT Question: “S.1.2: What impact would there be on the solution if the Federal Reserve required it to settle in central bank funds?

OUR Answer: “Settling in central bank funds will require additional 33% more messaging and mapping to Fed accounts. InterComputer’s Patent Claims 6 and 12 (included in Addendum B in the original Proposal) cover this possibility.”

JUSTIFICATION: If necessary, mapping to the Fed account system would be a one-time process. Settling in Fed funds would have zero impact on the safety, security, or insured nature of the TSS system.

QIAT Question: “S.1.2: In a model where every bank has a correspondent, bilateral TSS account with every other bank, how would ICN manage systemic risk?”

OUR Answer:

- All systems nodes are of equal strength.
- Payments causing even a hint of a problem are halted instantly for review.
- Banks may instantly revoke, suspend, and reinstate the digital certificates of any of its users.
- Please refer to the detailed answer to question S.4.1.

JUSTIFICATION: Pages 5 – 8, and Addendum A, of our Proposal describe the management of systemic risk in the TSS system in detail, including these three critical areas:
- The inherently unsecure nature of the message pathways employed. (JUSTIFICATION: The fact that our solution never touches the World Wide Web eliminates all web-related systemic risk.)
- The necessity of manual human intervention to complete some transactions, especially when multiple legacy systems must be used for one transaction. (JUSTIFICATION: The IC IOS automatically enforces in every message all layers of abuse detection, microburst tunneling, potential abuse detection, and continuous machine and data audit, to protect the attributes of identity/authority management. This process is not subject to manual human intervention. This process works consistently throughout the entire system, thus preventing this type of systemic risk.)
- The relative ease with which user identity/authority credentials can be abused for fraudulent/criminal purposes. (JUSTIFICATION: Identity and credential spoofing by unauthorized actors, such as the type that breached and plundered SWIFT, is inherently more risky on a real-time payment system. That is why the IC IOS and the TSS system were designed from the ground up to eliminate such risks. Our success in doing so is evidenced by the transaction insurance underwritten after more than a year-long evaluation by our insurers.)

Finally, the TSS system employs offsite, hot site, mirrored backup to prevent the systemic risk associated with down time. This backup is a condition of our transaction insurance coverage.

QIAT Question: “S.1.2: How extensive is the insurance arrangement with Lloyds? Are there any settlement-related situations that are exempt from coverage? If so, what are they and how are they handled? What are the specific credit and liquidity risk exposures associated with these?”

OUR Answer: Pages 11 – 16 of our Answer document provide a detailed description of residual risk and include detailed policy provisions of our e-Comprehensive transaction insurance.

JUSTIFICATION: In the absence of underwritten insurance coverage, who will pay for the losses from residual systemic risk? The banks? Which other proposer offers such loss coverage end-to-end? Should something go wrong, does the QIAT truly think that banks will prefer to cover their own losses instead of collecting insurance payments to make them whole? This feature alone deserves a higher QIAT rating.

QIAT Question: “What if the ICN’s insurance plan is not available in the market at reasonable prices in the future (what are the arrangements for its renewal and at what terms)? How will the cost of the insurance be covered in future years when the Solution is running at scale?”

OUR Answer: “Industry experience with eComprehensive policies since 1985 to date has seen only a strong increase in such underwriting activity. Significant volume increases should drive costs down for insurers.”

JUSTIFICATION: Thirty years of market history and experience gives us no reason to think that the underwriting of electronic data policies will do anything other than increase as increasing volume drives prices down and policy limits up. Our arrangements provide for annual renewals. The insurance is available through U.S.-based companies as well as Lloyd’s.
Section S.1.3 – Operational Risks

CRITERIA: S.1.3 Address operational risks due to systemic deficiencies, human error, management failure, and external disruption.

QIAT Question: “S.1.3: Are participating banks required to meet SLAs for network availability? What are the minimum/maximum requirements in these SLAs? Are there any penalties for missing availability targets?”

OUR Answer: “InterComputer is committed to a 99.9% availability via offsite/hotsite mirrored capability. We will require the same of banks that participate in the ICN and we can provide offsite/hotsite mirrored services to those who prefer it.”

JUSTIFICATION: Banks are responsible for the uptime of their respective customer account systems. InterComputer can offer uptime support resources to banks if desired. We have not provided copies of the SLAs to the QIAT because of the proprietary nature and commercial value thereof. If any task force member will sign an NDA, we will make them available for inspection.

Section S.1.4 – Fraudulent/Erroneous Payments

CRITERIA: S.1.4 Address operational risks related to deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events (see S.8).

QIAT Question: None.

OUR Answer: None.

JUSTIFICATION: In the absence of a question, we assume the proposal was effective in addressing this issue.

Section S.1.5 – Risk Containment Incentives

CRITERIA: S.1.5 Include incentives (i.e., positive, negative, financial, or non-financial) to operators and Providers to address and contain risks they pose to other Participants.

QIAT Question: None.

OUR Answer: None.

JUSTIFICATION: In the absence of a question, we assume the proposal was adequate in addressing this issue. Our expectation is that banks will find the fee opportunities associated with delivering the substantial added value of insured secure transactions to be a more than adequate incentive to control any risks they may pose to other participants.

Section S.1.6 – Periodic Review and Update

CRITERIA: S.1.6 Be subjected to periodic review and update.

QIAT Question: None.
OUR Answer: None.

JUSTIFICATION: As we stated in S.11.3:

S.11.3: What monitoring processes does ICN employ to ensure FI compliance with its participation requirements and how does it enforce these requirements?

☐ A security review is required at the time of setup.
☐ An annual security audit is also required.
☐ TSS system is constantly monitored for overall system compliance and around the clock staff attention by InterComputer.
☐ All messages are automatically subjected to ICN and user company policies at all times.

Unlike PCI standards, we have already stated that our solution uses automatic enforcement.

In the absence of a question, we assume the proposal was adequate in addressing this issue.
Section S.3 – PAYMENT FINALITY

OUR Rating: Very Effective

QIAT Rating: Somewhat Effective

Section S.3.1 – Account Provider Approval/Good Funds

CRITERIA: S.3.1 The Solution should require the Payer’s Depository Institution or Regulated Non-bank Account Provider to approve each payment following payment Initiation to assure the Payer’s Account has Good Funds. Note: In assuring Good Funds, the Solution should foster Consumer control and understanding of Account management implications and any related fees; the permissibility of overdrafts should be decided by an appropriate regulatory authority and the Solution should demonstrate compliance with all regulatory guidance related to overdrafts and credit, as applicable.

QIAT Question: None.

OUR Answer: None.

JUSTIFICATION: Pages 22 – 27 of our Proposal describe the payment and settlement process, which includes an automatic feasibility request at the point of payment initiation. Once sufficient funds are confirmed, the transaction proceeds.

Section S.3.2 – Payment Irrevocability/Legal Framework

CRITERIA: S.3.2 The Solution should architecturally enable, and have rules and/or a supporting Legal Framework that clarifies exactly when the payment becomes Irrevocable, but this should be after Good Funds Approval and no later than when funds are made available to the Payee. The exact point of Irrevocability should be easily understood by and visible to the Payee (see F.5).

QIAT Question: None.

OUR Answer: None.

JUSTIFICATION: Addendum C of our Proposal describes the two-step confirmation process required to initiate a payment.

The first confirmation screen is embedded in the payer side of the system. The second acceptance screen is embedded in the bank side of the system. This architectural requirement, combined with the legal terms of the SLAs, deliver full legal payment finality. As previously stated,

Section S.3.3 – Disputed Payment Protections

CRITERIA: S.3.3 The Solution should provide mechanisms and processes to protect or compensate the Payer in the event that the payment is disputed and to comply with relevant Consumer protection regulations, including Regulation E (see S.5 and L.1).

QIAT Question: Will ICN develop a dispute resolution process if participating banks require it? If not, what would the Solution offer instead?
OUR Answer: ICN can offer a “dispute resolution” process if banks require it. Nevertheless, we think banks could profit from forgoing the expenses associated with “unwinding” real-time electronic payments. If any task force member will sign an NDA, we will make the SLAs (which contain the detailed legal underpinnings of the payment process) available for inspection.

JUSTIFICATION: ICN can offer a “dispute resolution” process if banks require it. For example, if a payer selects an unintended payee for a payment, they may call their bank and have the payment unwound if the bank agrees to do so. Our solution is fully compliant with Reg E.
S4 CRITERIA- SETTLEMENT APPROACH

OUR Rating: Very Effective

QIAT Rating: Somewhat Effective

Justification for S.4:
PL Payments Legal Framework, applications, processing systems, and transaction insurance combine to deliver real-time payments that are cleared, settled, and legally final in less than 15 seconds. There is no lag time or risk. Good funds are debited upon payment instruction from sender. At that point the funds are sent to the recipient in 15 seconds with absolute legal finality and immediate funds availability.

The justification for the QIAT’s rating is unclear.

CRITERIA: Section S.4.1 – Settlement Obligations and Requirements

The Solution’s rules should define when and how Depository Institutions and Regulated Nonbank Account Providers settle obligations to one another arising from End User payments (e.g., Real-Time gross Settlement, deferred net Settlement, frequency of Settlement, hours of Settlement operation, etc.). The Solution’s participation requirements should be designed to ensure that compliant Depository Institutions and Regulated Non-bank Account Providers have the operational, financial, and legal capacity to fulfill their obligations, including to other Providers, on a timely basis. Where a Depository Institution or Regulated Non-bank Account Provider settles on behalf of others, it may be appropriate for the Solution to impose additional requirements to ensure that the settler has the financial and operational capacity to do so.

QIAT Question: The ICN describes in detail how it transmits clearing messages and the rules that govern funds’ irrevocability and timing. Please describe in equal detail how funds are settled between the payer FI and Payee FI within the TSS.

OUR Answer: A detailed explanation of the functionality of the Trusted Settlement System (TSS) follows. It is presented here, in full, only once out of respect for the reader’s time. Answers to other questions may simply refer to this section.

Trusted Settlement System (TSS)

The payment clearing and settlement process and the actual movement of funds occur together in the Trusted Settlement System as defined on pages 24-27 of the proposal. The ledger on page 26 defines the debit/credit clearing and settling process at each phase of the money movement between banks in commercial funds.

To understand the movement of funds for settlement, it is important to note that every payment initiated by any bank customer first much pass a feasibility test (step 1 in the ledger on page 26), which queries the DDA account to ensure sufficient funds to make the payment. If the funds are sufficient to make the payment, the payment process continues to completion. If the funds are not sufficient, the payment cannot begin to go forward and the payer is so notified.

The process for clearing, settlement and movement of funds is:

If funds are sufficient to make the payment, the money is debited from the customer DDA account at that moment.
The bank correspondent account is not like a traditional correspondent account; it is better labeled as a Correspondent Bank Settlement Account or simply a TSS settlement account.

The debit from the customer DDA account is the money, which is set aside to move along the clearing path to the payee’s bank account after all debits and credits have been applied perfectly in the TSS system.

If there is any problem with the messaging concerning debit and credit conditions, e.g. if an imbalance should appear at any time, the money stops with the messages and entries and reverts back to the customer DDA at the payer bank.

Should a message or acknowledgement fail, or if a debit/credit imbalance is flagged and sent as an alert to authorized bank personnel for review.

In this event, the original message is sent through an alternative microburst tunnel. If this second attempt fails for any reason, the money reverts immediately back to the payer’s DDA account and the situation is flagged for further review.

Please follow the flow on the ledger on page 26 of the proposal. There are 12 steps of debits and credits which must be equal in both the send messages and acknowledgement messages.

The “Yes” column in the ledger on page 26 represents that the send and acknowledgement messages have succeeded, and that the debits and credits represented in the “Amount” remained the same from end-to-end.

Continuous Message Audit is active throughout the system and ensures that the messages and acknowledgments have not been altered in any way.

Once all messaging is complete, the money has moved and the payment is legally and finally settled.

There are no compensating balances as in traditional correspondent bank relationships to keep on account at correspondent banks.

Although the debits and credits are flowing through the system at any given point in time, if payments ceased and all active messages completed, the overall balance in the TSS accounts is always zero. Debits and credits always cancel each other out.

We recognize that there are other accounting entries involved with customer deposits and disbursements on the backend of the bank accounting systems. During the requirement gathering process to integrate to the customer account system, these accounting entries are evaluated and the mapping procedures modified to fit the requirements of each bank.

Clearing and Settlement with Federal Reserve Funds Option

Our patent claims per the proposal include settlement through third party financial institutions such as the Federal Reserve. If, for any reason, the banks and the Fed determine that payments should be settled in Federal Reserve Funds, it will be necessary to map the TSS system to bank’s Federal Reserve account.

The impact of this method is that a set of payment request and acknowledgement messages are sent to bank’s Fed account and a set of payment messages and acknowledgments from the bank’s Fed account back to the bank for posting to the bank’s customer account.
This method adds one-third more messages in the end-to-end process and approximately five additional seconds to the overall average payment speed. But the TSS design accommodates this option with ease. Certainly, additional mapping is required.

**TSS Availability to Third-party Non-Bank Providers**

Our patent claims cited in the proposal accommodate the potential of third-party, non-bank providers (e.g. qualified money transmitters and even credit companies) should the business case warrant it. It’s important that the business conditions remain neutral or advantageous to our bank customer. The approximately 8,000 banks and 3,000 credit unions in the United States are our first priority.

In many cases, banks may benefit from the inclusion of large, third-party, non-bank providers as they all must have bank accounts too. If anti-trust requirements of legislation should mandate inclusion, the TSS system is designed to be inclusive.

From a process standpoint, adding non-bank providers is similar to moving payments through the Federal Reserve. The third party non-bank provider must be provisioned and set-up on ICN. Mapping requirements must be defined and of course, it also adds a third set of messages and acknowledgments. It will add about five seconds to payment completion time.

**JUSTIFICATION:** Pages 24 – 27 of the Proposal and pages 18-19 of the Q&A document describes the settlement process in detail.

The three most important points are:

- There is a feasibility request at the time the payment is attempted. If there are good funds, the money is debited from the payer DDA account. Otherwise, the payment process stops.
- Every message in the IC IOS must have a corresponding acknowledgement message returned to the system unchanged.
- Debits and credits throughout the system clear with all corresponding acknowledgements at each of the six transaction stages. As all debits and credits are reconciled and acknowledgements received, the money is transferred at the same time. When the final acknowledgement occurs, the entire transaction is considered final both technologically and per the bank agreements. The money has been cleared and settled simultaneously, and is immediately available for the payee’s use.

**CRITERIA:** S.4.1: Have you confirmed that transaction insurance be sufficient to satisfy FI risk departments?

OUR Answer: Yes. Please see the detailed answer to S.1.2 concerning Transaction Insurance.

**JUSTIFICATION:** As the system grows, the transactions limits still apply. We have not confirmed with banks what their transaction coverage should be. No other entity can provide this same coverage which puts InterComputer’s solution head and shoulders above any other in this regard.

**QIAT Question:** S.4: How do you propose that FIs manage settlement accounts across potentially thousands of FIs?

OUR Answer: Each FI has only one TSS settlement account, which is established at contract signing. Each FI has full view of any payment to which they are a processor/party at all times throughout the entire ICN network.
JUSTIFICATION: With 8,000 banks and 3,000 credit unions in the nation, and the current state of IT capability, processing the Fed’s 2012 estimate of 4.5 million hourly ACH/check image payments is a very finite proposition. (It averages about 400 transactions per hour per FI.) InterComputer’s software scales to meet higher demands and hardware and Internet bandwidth are more than adequate.

QIAT Question: S.4: What visibility will be provided to FIs to monitor and manage these account balances?

OUR Answer: The mapping of each FI’s internal account management systems to the ICN provides all required visibility.

JUSTIFICATION:

QIAT Question: S.4: As the number of FI participants increases, settlement accounts will need to be funded in near real time to ensure end users can transact.

OUR Answer: There is no funding required for TSS settlement accounts, ever. The TSS settlement accounts are designed to always have a zero balance when not executing a transaction.

JUSTIFICATION: The money moves with the debits and credits and requires no compensating balances in any kind of settlement account. What can be more efficient and effective than this approach?

QIAT Question: S.4: What funding options are available to FIs?

OUR Answer: N/A

QIAT Question: S.4: What collateral options are available to FIs?

OUR Answer: N/A

QIAT Question: S.4: What happens if an FI in the system fails?

OUR Answer: The Fed monitors FIs equity and liquidity levels continually. InterComputer will comply with any Fed directives to revoke any FI’s access to the ICN/TSS system. Upon notice of failure, InterComputer, or the issuing digital certificate authority, will immediately revoke the bank’s identity/authority certificates, thereby preventing the bank from conducting any further operations on the system.

JUSTIFICATION: We will arrange with the Fed to be notified if a Bank is falling short of regulatory compliance and requires action on our part. A troubled bank may still be able to engage in this process based on individual circumstances.

Section S.4.2 – Risk Management Framework/Liquidity and Credit Concerns
CRITERIA: Provider credit and liquidity risk exposures arising from any lag between transaction Finality and inter-Provider Settlement and to ensure that credit exposures to each Provider can be fully covered. Any special credit and liquidity risk considerations for a Solution that is available to End Users on a 24x7x365 basis should be addressed.

QIAT Question: None.

OUR Answer: None.

JUSTIFICATION: We will arrange with the Fed to be notified if a Bank is falling short of regulatory compliance and requires action on our part. A troubled bank may still be able to engage in this process based on individual circumstances.

Section S.4.3 – Settlement Monies Central Bank/Commercial Bank

CRITERIA: The Solution should either enable Settlement in central bank money, or minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money for the inter-Provider Settlement process.

QIAT Question: None.

OUR Answer: None.

JUSTIFICATION: InterComputer can work with the Fed to develop a mechanism to deal with banks that fall in this category.
CRITERIA: Fraud information sharing means that the Solution should require and facilitate timely and frequent sharing of information among all Providers, operators and regulators to help them manage, monitor, and mitigate Fraud and evolving threats in accordance with applicable law (see L.4).

OUR Rating: Very Effective

QIAT Rating: Somewhat Effective

Justification for S.6:

The ICN is currently very effective at satisfying S.6.1 through S.6.7 because the mere sharing of fraud information via a centralized repository has no effect on real-time payments. ICN’s digital identity/authority certificates, multiple layers of protection (including abuse and potential abuse detection), TSS operations and full value transaction insurance all work together to prevent fraud in real-time. Should a number of incidents become sufficient to indicate a fraud pattern, any user’s digital credentials can be immediately suspended or revoked by the issuer to preclude any further incidents. (S.7.3) Sharing any generalized form of technological fraud information (beyond the identity of the perpetrator) with non-real time systems would have little to no value in preventing future fraudulent actions. The nature of the ICN makes all such information sui generis.

Section S.6.1 – Fraud Information Sharing

CRITERIA: The Solution should require the sharing of information to facilitate managing and monitoring Fraud (e.g., patterns suggestive of risk, known instances of Fraud, known vulnerabilities, the significance of the information and effective mitigation techniques). Information shared for anti-fraud activities should be used only for fraud management purposes. Whenever possible, personally identifiable information should be excluded from information sharing. If shared, © 2016 Federal Reserve Banks. Materials are not to be used without consent 19 such information should be encrypted (see S.9 and L.4).

QIAT Question: None.

OUR Answer: None

Section S.6.2 – Data Aggregation for Fraud Information Sharing

CRITERIA: The Solution should describe how Data owned by Entities other than Providers and operators would be aggregated, managed and protected for purposes of Fraud information sharing.

QIAT Question: None.

OUR Answer: None

Section S.6.3 – Real-time Management and Monitoring of Fraud

CRITERIA: The Solution should facilitate information sharing that supports Real-Time and ex-post management and monitoring of Fraud, and provides timely updates and alerts.

S.6.3: Would the ICN consider the creation and/or management of a centralized fraud monitoring capability that monitors transactions and end user data in the TSS and is shared (as appropriate and if needed) to identify potential trends? This might even be handled by a third party.
The system already contains a centralized abuse/fraud rules and the captioned monitoring capability system wide. In effect, the system provides fraud information sharing in real-time.

JUSTIFICATION: Please refer to items L.2.2 and L.3.3 in the Q&A document concerning a bank-run committee that could review fraud/abuse rules to be pushed out to all banks on the system. The same committee could recommend changes/additions to the SLAs that govern system participation.

Section S.6.4 – Information Sharing Mechanisms

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

QIAT Question: None.

OUR Answer: None

Section S.6.5 - Information Sharing Roles/Responsibilities

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

QIAT Question: None.

OUR Answer: None

Section S.6.6 – Central Fraud Information Repository

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

QIAT Question: None.

OUR Answer: None

Section S.6.7 – Fraud Pattern Recognition

CRITERIA: The Solution should have the ability to aggregate Fraud information to spot patterns that may not be visible at the level of an individual Participant.

QIAT Question: None.

OUR Answer: None
F1 CRITERIA- FAST APPROVAL

CRITERIA: Fast Approval means that the Solution should require and enable the Payer’s Depository Institution or Regulated Non-bank Account Provider to assure Good Funds for each payment in a timely manner, as indicated by the effectiveness scale below.

Note: This criterion is measured from the completion of payment Initiation (just following Payer Authorization to their Provider, or just following confirmation by the Payer’s Provider that pre-authorization exists for a given payment) to the point when the Payer’s Depository Institution or Regulated Non-bank Account Provider approves or denies the payment.

Very effective – Within 2 seconds.
Effective – Within 5 seconds.
Somewhat effective – Within 15 seconds.
Not effective – Over 15 seconds.

QIAT Rating: Somewhat Effective
OUR Rating: Very Effective

Justification for F.1:
PL Payments meets or exceeds the shortest time criteria for this step. We wrote the book on (and have the patent for) real-time payments.

JUSTIFICATION: The rating criteria listed above compare apples to oranges in the case of InterComputer. The 15-second payment cycle time we have demonstrated INCLUDES real-time clearing and settlement, with immediate funds availability and payment status visibility. (Criteria F.2 through F.5) The criteria listed above clearly apply only to approval and posting, with clearing and settlement occurring at some later time.

Please not the following inconsistency in the QIAT Ratings:
In section F.1 and F.2, “Fast Approval” and “Fast Clearing” are rated as “Somewhat Effective”.
Yet, in section F.3, “Fast Availability of Good Funds to Payee” is rated as “Very Effective”.
F.3 cannot, by definition happen any faster than F.1 and F.2.
The proposer submitted questions (on previous pages) to the QIAT after receiving their Draft Assessment. The QIAT sent the following response to the proposer.

September 29, 2016

Thank you for your concerns. As you are aware, all proposals are evaluated relative to a standard framework constructed by the Faster Payments Task Force. The framework supports the evaluation of proposals on several categories, focusing heavily on the impacts to end users and the delivery of a consistent experience. With regards to your proposal, there are three areas where the QIAT has concerns: The need for insurance to manage risk created by the solution; the settlement process described in the solution; and the lack of formal dispute management process. Please see our responses below to your specific points:

S.1 Risk Management
QIAT concerns in this category are as follows:
1) The proposal does not provide any documentation regarding a formal process to handle errors, exceptions or disputed payments.
2) The settlement process described in the solution does not address the movement of commercial funds between banks to support transactions that occur in the TSS.
3) Risk management policies should target the avoidance of systemic incidents and outline processes to address these. While an insurance policy has true value in compensating individual loss cases, it is not considered sufficient to address settlement risk, due to the time and possible extent of the impact of an incident. As such, while the described insurance policy is valuable, it is not considered an alternative to policies that manage settlement risk.

S.1.3 Operational Risk
The materials indicate that InterComputer commits to 99.9% availability. The solution would be enhanced with a description of how 99.999% availability can be delivered.

S.1.5 Risk containment incentives
Rather than relying on an expectation of what banks will do, the solution should clearly describe all participation requirements and payment system rules, and any penalties for non-compliance with participation requirements and payment system rules.

S.3 Payment finality
The rating reflects the lack of a dispute process. Since this is an end-user-focused view, the dispute process is an important aspect of any solution.

S.3.3 Disputed payment protections
The evaluation criteria clearly requires a dispute resolution process. The proposal indicates that users will be directed to their banks. It would be preferable to see evidence of a dispute process that is clearly defined, applicable to all providers of the solution, consistently applied across providers to deliver a consistent end user experience, and transparently communicated to end users regardless of the provider. Although the QIAT understands that the solution reflects the requirements of Reg E, it is not clear from the material provided how the solution will provide mechanisms and processes to protect or compensate the Payer in the event that the payment is disputed.
**S.4.1 Settlement obligations and requirements**
The QIAT has carefully reviewed all of the information provided. There are outstanding concerns about the settlement as described. The solution does not describe the settlement of commercial funds. Transaction and balance information moves between TSS accounts in real time, and the credit and debit mechanism will result in a zero balance within TSS accounts. However, TSS settlement does not appear to be equivalent to settlement in commercial funds, requiring the actual transfer of fiduciary funds. In order for the transaction to settle, the commercial currency that was debited from the payer's account and credited to the payee's account should be accounted for using commercial money settlement mechanisms. The solution would be enhanced if it were implemented using a settlement option in which transactions were settled using a Fed account.

**S.6 Fraud information sharing**
The solution does not satisfy the FPTF effectiveness criteria for fraud information sharing. The materials state that the solution does capture all of the information, and it was stated in the Q&A response that the solution provides fraud information sharing in real time. However, the proposal does not describe what information is captured, what information is available to participants, what information is aggregated at an industry level (if any), or how it this information is shared. Further details would enhance the solution.

**F.1 Fast approval**
The materials describe the process end-to-end as taking 15 seconds: a detailed breakdown of this timeline is not provided. Based on the information provided, the QIAT has evaluated the solution as SE based on the 15 second data point. It is the QIAT's interpretation that the 15s cycle time means that the solution will make funds available within the threshold stated in the requirements as VE for F3. However, no detail is provided on how fast approval and clearing would take place, which leaves the QIAT with only the 15" range to evaluate the entire completion. For F1 and F2, these 15s are equivalent to an SE rating. The QIAT is bound to compare the proposal to the Faster Payments Task Force individual criteria. While we acknowledge that the end-to-end payment cycle merits a VE rating (as in F3), the description provided for the sub-components for approval and clearing (F1 and F2) do not meet the criteria for a VE rating.

The criteria for F3 - availability of funds - are described below. The solution delivers available funds in less than 1 minute and earns a VE rating.

- **VE** - 1 minute
- **E** - 30 minutes
- **SE** - 60 minutes
- **NE** - more than 60 minutes
Faster Payments QIAT

PRELIMINARY ASSESSMENT

Proposer: InterComputer Corporation

Description of Solution:

The InterComputer Network (ICN) is an end-to-end payments, Internet protocol-based solution that supports real-time payments. By relying on its own operating system in a closed network and layering this with additional security, it provides a secure environment for payment delivery. While it is IP-based, the solution is not accessible via the World Wide Web and therefore is protected from the risks that that presents. ICN manages user identities and authority with proprietary digital certificates. It enforces these with three-factor end user authentication that includes user name and password, digital certificate, and biometric validation (which increases the security of the solution, but also increases end user actions needed to authenticate each and every payment).

The solution requires two contracts to be in place to support enrollment: one between the bank and ICN, and one between the bank and its customers/end users. Banks that wish to participate in the solution must install the ICN’s operating system and its Trusted Settlement System (TSS) application. The solution relies on the relationships between all participating banks to support real time settlement through the establishment of a new ‘correspondent bilateral system’ between all banks that wish to be in the system. End users can access the solution through an application called Private Line that allows for interaction with the ICN through a smartphone, tablet, or PC. Private Line includes PL Pay (which supports all transaction types) and eCash (which links FIs and their customers). End users’ payments within ICN are validated, cleared, and settled within 15 seconds. These payments are all irrevocable credit push payments.

EXECUTIVE SUMMARY OF THE PROPOSAL

**Major strengths**

- The ICN is a very secure solution and operates as a closed loop system on a private network. Payment transactions require three-factor authentication to support initiation (i.e., user name and password, biometric confirmation, and the digital certificate that is unique to the end user). Payers must also confirm a payment prior to sending and review terms and conditions for every transaction. All payments are push payments and irrevocable. The solution is insured by Lloyds of London.

- The solution’s flexibility also supports many useful features. It allows end users to make exchanges across several interfaces and to set up a hierarchy of accounts for making payments. If the preferred account is short of funds, ICN moves to the next account to complete the transaction, although it does not address what authorizations would need to be obtained for this. As a closed network it can also monitor the status of payments very efficiently. By relying on the Application Program Interface (API) for integration, the solution can work with treasury management, accounting systems, ERP systems, and small business systems (e.g., QuickBooks). Its messaging format leverages ISO 20022. This flexibility – as well as ICN’s scalability – offers significant potential for customization.

**Areas for improvement and enhancement**

- Broad deployment in a reasonable time frame (18-30 months) will require strong regulatory impetus from the Federal Reserve and other banking regulators (p. 41) and seems doubtful.
– The solution does not offer a governance framework and proposes that if governance is required, it should be provided by government regulators such as the Federal Reserve, FDIC, and OCC (page 57).

– The solution does not outline how the deployment and operation of this new payment system will be funded, and clarification of costs to be incurred by participating FIs and end users is needed.

– The customer experience in the ICN seems quite burdensome. To enroll in the solution, consumers have to receive a CD or USB stick with the Private Line application in the mail. They must authenticate themselves for every transaction with a biometric identifier and a password. Transactions must be confirmed two times before sending, regardless of type or value of the transaction. The ICN also limits end users who can use it because it is a bank-account to bank-account solution; it does not address the unbanked.

– The solution does not settle in central bank funds, but rather re-uses commercial bank funds exchanged between participating FIs.

– ICN does not appear to adequately address risk management, and gaps exist in its legal framework. The solution does not consider exceptions and dispute handling. There are insufficient details outlining how the solution would store and share fraud information, and how it would deal with a security breach. The proposal states that presenting the terms and conditions twice during every payment process will eliminate any transaction risk that is related to errors. Any disagreements that cannot be settled amicably are to be addressed outside the payment system by using the court system. The evaluation criteria suggest a more formal dispute process is preferred.

■ Use cases addressed

■ Proposer’s overall ability to deliver proposed solution
– The value proposition for FIs is not as compelling as needed to support the target market share provided in the proposal. It is likely that, as stated in the proposal, a strong regulatory impetus will be required to support adoption. The implementation timeline is extremely aggressive and does not consider the complexities of design and implementation with numerous banks required for ubiquity.
Ubiquity

U.1 Accessibility

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The ICN is accessible to customers of any enrolled bank or credit union. It uses an Application Program Interface (API) to support the FI’s enrollment, and that of their customers. The solution can also initiate payment instructions with ACH and Fedwire,

End users whose banks do not participate in ICN cannot register. They must change FIs to a bank that is participating in the system. End users can register with ICN directly, but can only transact with other directly-registered users. For these users, the available transaction set is limited and payment instructions related to sending and receiving payments are processed using an ACH network (U.1.2, U.1.4). The driver for customer adoption will include avoidance of the risks and cybercrime associated with web-based online banking. One of the motivating factors for FIs to participate will be a reduction in the high costs associated with securing web-banking solutions, and the ability to offer customers ‘the ultimate’ in digital security. The proposal states that FIs are spending “vast sums of money attempting to secure completely unsecurable, web-based online banking.” The proposer states the installation of ICN’s PrivateLine software virtually eliminates these costs. Any additional drivers of FI adoption should be clearly described.

The implementation timeline described in the proposal is aggressive – 18 to 30 months. The proposal acknowledges that the proposed timeline is only achievable if a strong regulatory impetus is provided by the Federal Reserve and other regulators (p.40) (U.1.5).

U.2 Usability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
There is substantial setup required for banks that wish to participate in the solution. Banks must implement ‘PrivateLine Control Bridge’ to provision employees with digital identity certificates and authority within the solution; provision customers and determine authorities; and provision applications that will be used as part of the solution. It is challenging to set up the existing user base for the first time to generate digital authority certificates. Conversion of an existing customer base to PrivateLine can be implemented branch by branch. Once created, certificates are easily modified to reflect any changes in information, accounts and authorizations.

For end user registration, the bank sends the client side of PrivateLine in physical media format (CD, USB key or Micro SD card) via postal mail. Web-based download is not permitted. The ICN is accessible via multiple devices (computer, tablet, and smartphones) through the PL application. The solution is available 24/7/365. All transactions are push transactions, end users must accept terms and conditions for every transaction. Connections between end users are established through a connection request sent to another individual or an entity. Entities can determine how they can be searched on the system. Connection requests must be accepted by the receiver before payments can be exchanged. An entity’s “real name” is the primary attribute for searching, connecting and paying, but email addresses or telephone numbers can be added to the profile if desired.
The end user authentication and transaction approval requirements result in a lengthy payment experience and may inhibit some end users from using the ICN. The system also provides notifications.

**U.3  Predictability**

<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 ICN is a fully detailed, secure, and controlled payment process with disclosure. It also supports a consistent end user experience across channels. The same user interface and the same payment processes (from initiation to settlement) occur for every transaction. The end user application is “Private Line,” and “PL Pay/payment” is the branded solution.

The proposal supports the sharing of fees associated with a transaction through the use of a configurable field, or by adding language to the acceptance screen, but there is not a requirement to inform end users about fees before the payment occurs (U.3.2).

There are no error protection rights described in the solution. Disputes that cannot be amicably resolved between the payer and the payee must be settled outside the payments system in the courts. The ICN also does not allow payment repudiation (p27) (U.3.5). The proposer describes that ICN can offer a ‘dispute resolution’ process if banks require it.

The solution’s name is “PrivateLine Payments”. A Private Line label or icon will be available for merchant locations to inform end users that they can make real time payments at that location.

**U.4  Contextual data capability**

<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 ICN allows the exchange of contextual data in all of its transactions. Associated messages, regardless of format type, arrive in real time with the payment message. Enrolled business users, for instance, can connect their accounting/purchasing systems to IC and initiate PL Payments directly from their business application. Business partners can leverage an InterComputer solution called PrivateBusinessDrive to exchange large contextual data files independently of the payment. The solution states that all messages within the ICN use ISO20022 XML syntax. The proposal states that mapping to non-standard applications can be developed in weeks if this is required as part of contextual data for payments.

**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 ICN currently views cross-border functionality as both a mid- and a long-term priority. In the mid-term it can extend the TSS to international banks, and leverage the same legal agreement. The solution does support payments made in currencies other than the U.S. dollar.
Large banks dealing in multiple currencies can send or receive payments directly with international banks that also use PrivateLine. IC will need to develop greater pricing and conversion transparency for its international end users (U.5.3). Over the longer-term, the solution proposes to build direct TSS and banking relationships with global banks and will share fees with them.

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>
<tbody>
<tr>
<td>Rationale:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The ICN supports all the use cases, including B2B, B2P, P2B (including POS), and P2P.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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>
<tbody>
<tr>
<td>Rationale:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any bank or credit union can participate in the solution as long as they sign the required agreements, implement the TSS capability, and join the Payment Legal Network. If the FI does not want to implement the TSS, ICN can host it for them.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The proposal states that FIs can brand and price PL Payments without any constraints defined by InterComputer. There are a number of parameters that are defined by the individual FIs in their implementations of Control Bridge and deployment of the solution (account types, transaction amounts etc.), but the end user experience and access to the system seems to be very tightly controlled by ICN and supported by standard agreements to be signed by all participants. If an end user wishes to change banks, their digital identities are revoked by the first bank, and they must be registered by the new bank to receive a new digital certificate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The proposal indicates that an InterComputer SDK is available to adapt existing solutions to the ICN, or create new solutions that can be integrated with the ICN. The process for the integration of new services is not described.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The solution can support the disclosure of fees in advance of a transaction, but does not require this disclosure. There is a configurable field that can be used to display fees in advance. Alternatively, fee information can be added to the legal language that is presented on the transaction acceptance screen.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC allows enrolled FIs to develop and offer additional value-added services to their customers. The ICN Software Developer Kit provides gateways for providers and other software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
developers to create applications that run on the IC IOS. In the proposal as written, it does not appear that non-banks are able to develop value added services. The proposal states that the optionality of value-added services and the disclosure of any fees is the responsibility of the service provider (E.2.3).

E.3  Implementation timeline

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

**Rationale:**

The solution outlines an implementation plan that is very aggressive. The 18-month timeline allotted for the key activities for each FI may not be sufficient. Details are not provided for each major activity. It is not clear how many FI participants are needed to deliver scale. Success will require a substantial network of participating FIs. The implementation plan states that FIs should absorb the implementation costs but does not quantify the investment required for an FI to participate.

The proposal suggests that within two years, the solution could have 25% market share, and within three years, 50% market share. It is indicated that market share refers to the number of banks participating in the system. These penetration numbers will be supported by IC integration teams that work with bank IT staff to define requirements and determine schedules. It is stated in the proposal that bank IT staff can train and provision branch employees without InterComputer assistance. The role(s) of business and operation staff in the deployment process should be added. To support community banks and credit unions, the proposal suggests that third party providers could act as integration partners. The implementation plan does not describe the development and implementation effort required to support settlement in this system. The creation of a new correspondent banking network will almost certainly be time intensive and will require investment and support from FIs.

The proposal acknowledges that this aggressive timeline is only achievable if a ‘strong regulatory impetus’ is provided by the Federal Reserve and other regulators. Experience has shown that similar transformations – those that hinge on regulatory actions not currently under consideration – will require a much longer timeframe.

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 ICN leverages the ISO20022 standard for its transactions and applicable contextual data. ISO20022 is widely interoperable, can accept free text contextual data, is cost-effective, and is quite flexible. It is also developed and managed by the International Organization for Standards (ISO), a very well recognized body. The solution will provide flexibility to support multiple payment standards, and can develop new communication formats if needed to support contextual data needs.

E.5  Comprehensive
### Rationale:

Addresses and handles all aspects of the end-to-end payment process from initiation to reconciliation. The ICN’s technical design supports all of its features, including its information security protocols, compliance and risk controls, and reliability (among others).

#### 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 ICN’s distributed technology architecture makes it possible to scale its hardware and software globally as system volumes grow. IC’s hardware and bandwidth are the only things that limit its speed and usability. The proposal does not describe the solution’s capacity to handle projected volumes and values, projected throughput (TPS), or the impact of provider growth and transaction volume growth on transaction speed (E.6.2). The provider is committed to a 99.9% availability which is supported by offsite/hotsite mirrored capability. Any bank that participates in the solution is required to meet the same availability target. InterComputer can provide offsite/hotsite mirrored services for those banks that would prefer it.

#### E.7 Exceptions and investigations process

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

**Rationale:**

The solution has very thorough security and fraud prevention measures. By requiring payers to confirm payment details twice before executing the payment, the aim is to minimize transaction detail errors. There is no formal error resolution or dispute process for when errors occur and no tools or mechanisms are described that will assist in the resolution of errors or disputes. Lack of a dispute process may hinder adoption (E.7.1). The proposal indicates that a dispute resolution process can be developed if the banks require it.

IC stores all transaction information in the TSS Ledger and will retain information as mandated by the applicable financial regulatory agencies. The ICN does not aggregate information across providers in order to detect patterns (E.7.3).

### 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:
Overall, the solution relies on push payments, technology and authentication mechanisms to prevent risk in the system, and states that, as a result, very little systemic risk to no systemic risk will occur. The solution is flexible and can accommodate changes in law or legislation that impacted the solution.

The solution has no processes to handle exceptions or dispute resolution (S.1.4). Although the ICN plans to reduce operational risks through its distribution and technological setup, these measures do not credibly deal with all potential risks (S.1.3). The solution should include features to address payment-related risks including risks related to account set up, bilateral, non-collateralized settlement and denial of payments (S1.1-S.1.4). The proposal does not describe incentives for operators and providers to address and contain the risks they pose to other participants (S.1.5).

The proposal states that residual risks have been addressed through insurance coverage. A Transaction Insurance product was created for InterComputer and its customers in ~2005. This insurance protects “all organizations, employees, and customers of organizations which have been provisioned or registered to ICN according to established procedures and operation of the PrivateLine Control Bridge and ICN requirements”. Details of the insurance policy are provided in the proposal.

S.2 Payer authorization

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

Rationale:
The solution requires the payer to undergo three-factor authentication prior to initiating their payment, and they must review each transaction (with its terms and conditions) twice before sending it. The solution supports preauthorized push payments, but does not support pull payments of any kind. Once a payment is executed, it is irrevocable.

S.3 Payment finality

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

Rationale:
Each bank enrolled in the ICN signs the same enrollment agreement, which establishes three foundational obligations including agreement that every completed PL Payment is legally final, binding and non-rescindable, and that a participating bank will bind its customers to the same terms and conditions. They payment becomes irrevocable 10 to 15 seconds after the payer confirms the payment for the second time. There are currently no mechanisms defined to support a disputed payment (even one made in error) and the solution requires parties to settle their differences amicably. If the payer and payee cannot settle a payment issue, they have their only recourse is to the court system (S.3.3). The proposer has indicated that a dispute resolution process can be developed if required by the banks.

S.4 Settlement approach

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:
Every participating FI has a Trusted Settlement System (TSS) account. This account can be held by the FI on a TSS server, or the account can be managed by a third party on behalf of the bank. All payments in the system are push payments. The payments process involves confirming good funds are available in the payer’s DDA account, transferring the funds from the payer’s DDA to the payer bank’s TSS account, transferring the funds from the payer bank’s TSS account to the payee bank’s TSS account, and transferring the funds from the payee bank’s TSS account to the payee’s DDA account. All of these transfers occur in less than 15 seconds.

While settlement occurs in commercial bank money, the solution manages the risk through irrevocable push payments and legal agreements between the participants and end users. The solution can also support settlement in central bank money by mapping the TSS system to the bank’s Federal Reserve account. This implementation would require additional messaging and would add a few seconds (5) to the transaction time.

In the event that an FI in the system fails, InterComputer will immediately revoke the bank’s certificates preventing any further operations on the system.

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 ICN is designed to limit the occurrence of disputed payments, and the proposal as written does not define any role for itself in handling disputed payments. It denies any liabilities in this area because the solution trusts that the technology will avoid any such incidents. As a result, the proposal does not contain any procedures, mechanisms, or considerations for handling disputes or protecting business, government or consumer payers. Instead, the payer or the enrolled FI is responsible. The payer can request a voluntary return by phone, email, or chat platform. They have little recourse outside of regulatory compliance. The proposal does state that a dispute mechanism can be developed if required by the banks. It is suggested that a committee should be created to develop any dispute rules.

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 ICN believes that collecting fraud data in real-time systems is ineffective (p.29). Rather, if the system detects suspected fraud, it would immediately suspend the fraudulent user’s digital credentials. The ICN, the owner of the TSS, is the only entity currently able to monitor all transactions. The proposal states that the system already contains a centralized fraud monitoring capability, and, in effect provides fraud information sharing in real time. Rules can be added to the system as required and defined. The system does not provide any requirements for participating FIs to monitor their transactions for potentially fraudulent activity.

As the effectiveness criteria suggest, InterComputer may elect to reconsider its stance and develop or provide a monitoring capability to ensure that all end users and transactions in the solution are as expected.
S.7  Security controls

<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 provides a secure environment with multiple levels of security and encryption. The network has protected links and equally strong nodes. The secure message transfer system validates and exchanges secure messages in real-time. It also ensures an audit trail of all transactions. It would be beneficial if the solution defined minimum requirements for user enrollment to support providers. The technical security to support enrollment is unclear.

The proposal as provided does not define any requirements regarding server hardware. The core messaging software (i.e., IC iOS) will only run as fast as the available CPU power, memory, and storage space allows. It would be helpful for the solution to describe how participating FIs will manage and oversee the interface between the ICN and their existing risk management processes, other legacy payment infrastructures, and existing end-user interfaces.

S.8  Resiliency

<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 proposal indicates that the target availability for the solution is 99.9% which is delivered through offsite/hotsite mirrored capability. All participating banks in the system will have the same availability requirement. With regards to DRP and BCP, the solution states that InterComputer has BCP and DRP plans in place, and a system testing schedule as required by their underwriter. Participating FIs are required to have their own BCP and DRP for their nodes, and to comply with any SLA security practices. More detailed information describing the underwriters’ requirements and how these are satisfied would be helpful.

S.9  End-user data protection

<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 ICN requires operators and providers to use robust mechanisms (i.e., high-level encryption) to protect information (both end user and employee) in the end-to-end process. However, there do not appear to be similar requirements related to protecting the shared data (i.e., the ICN digital certificate) for the participating FIs. The proposal states that ICN requires operators to comply with data protection requirements as defined in the Service Level Agreement, but does not provide information as to what these requirements are.

S.10 End-user/provider authentication

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

**Rationale:**

The solution leverages ID verification (ID+V) and Know Your Customer (KYC) requirements for opening an account at participating FI. End users initiate all payments with three-factor
authentication, which requires their user name and password, biometric identification, and their digital certificate. The solution automates full compliance with relevant regulatory guidelines.

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 proposal indicates that any FI or credit union can participate in the ICN. The legal framework is set up through a law firm and everything is managed through a contract that is signed by every participating FI. Details are only available under NDA. When an FI becomes a participant, a security review is performed. Annual security audits are required. The TSS system is monitored constantly for overall system compliance by InterComputer.

**Speed (Fast)**

**F.1 Fast approval**

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

**Rationale:**
The solution takes somewhere between 10 and 15 seconds for approval. The Task Force’s criteria for fast approval is “Somewhat Effective” for anything within 15 seconds and over five seconds. “Very Effective” requires approval within two seconds.

**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 takes somewhere between 10 and 15 seconds for clearing. The Task Force’s criteria for fast clearing is “Somewhat Effective” for anything within 15 seconds and over five seconds. “Very Effective” requires approval within two seconds.

**F.3 Fast availability of good funds to payee**

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

**Rationale:**
The solution takes somewhere between 10 and 15 seconds for fast availability of Good Funds to the payee. The Task Force’s criteria for fast availability is “Very Effective” for anything within one minute.

**F.4 Fast settlement among depository institutions and regulated non-bank account providers**
Real-time settlement within the ICN, where the TSS exchanges commercial bank funds, would occur within 10 to 15 seconds. The real-time option is fully insured and must be available 24/7/365, which eliminates lag.

The solution suggests an implementation option that would map the TSS system to participating banks’ Federal Reserve accounts. This implementation may have a negative impact on the speed of settlement based on Fed operating hours.

**F.5 Prompt visibility of payment status**

**Rationale:**

The TSS notifies the payer and payee FIs as soon as their end users’ payment have been initiated and received. The FIs can then notify the payer and the payee; the ICN has not set requirements for the timing of end user notification.

**Legal**

**L.1 Legal framework**

**Rationale:**

The Legal Framework in Addendum C of the proposal describes how participants are legally bound to the ICN but does not cover some of the important areas in the FPTF framework. In describing how entities in the system will be legally bound, it appears that end users have no legal options on almost anything within ICN. The proposal describes which legal and regulatory obligations will govern the operation of the ICN. Compliance with many of these obligations are automated and automatically enforced by the solution. The solution’s SLA contains “terms and conditions of use, requirements for use, and the legal language to create absolutely, legally binding finality between banks and their customers that register for the solution. The proposal states that additional details regarding the solution’s legal framework are available under NDA.

**L.2 Payment system rules**

**Rationale:**

The proposal addresses key features of the solution, and describes obligations created by the legal framework. Addendum C summarizes the rights and obligations of the participating banks and end users, while the legal framework concentrates on payment irrevocability. There are no processes for error resolution. The proposal describes that a committee can be established to
address ongoing issues related to payment system rules (governance, abuse, regulatory concerns etc.). The committee would approve all changes, which would result in updating of software and SLAs as required and rollout to all participating FIs.

L.3 Consumer protections

<table>
<thead>
<tr>
<th>Rating</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td>Effective</td>
</tr>
<tr>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
Addendum C, which the ICN cites its source for consumer protection, summarizes the rights and obligations of the participating banks and end users; the solution’s legal framework concentrates on payment irrevocability.

It is suggested that the proposal allocate legal responsibilities for payer and payee losses in the case of disputed payments (L.3.1), and to establish payment system rules and procedures for error resolution (L.3.2). It should also consider setting up additional consumer protections and/or supporting payee and payer claims due to fraudulent activities or end user errors (L.3.3). In the event that consumer protection is required, the Bank TSS Committee will provide input and feedback. The TSS will be modified if required to deliver the additional customer protection requirements. Bank SLAs will also be modified.

L.4 Data privacy

<table>
<thead>
<tr>
<th>Rating</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td>Effective</td>
</tr>
<tr>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
The proposal states that PrivateLine and the TSS do not permit data collection. Data collection on personal or organizational transactions is not permitted. Payer or payee payment data is accessible only to the payer, the payee and their respective banks. Contextual data is only accessible by the payer and payee. If a government agency requires contextual or payment data, the request must be made using the required authorized legal documents. The proposal does not mention any policies on end users’ access to their own data, nor does it appear that an end user can limit the data/information collected on them or manage their own data privacy preferences. If a data breach is attempted, alerts are sent to all parties, and continuous system audit capabilities are engaged. The solution also seems to lack processes for surfacing, escalating, and dealing with a data breach (L.4.4).

L.5 Intellectual property

<table>
<thead>
<tr>
<th>Rating</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td>Effective</td>
</tr>
<tr>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
The solution has a clear proposed approach to resolve and manage any risks arising from third-party intellectual property rights (prior to implementation). The proposal described several patents and patents pending, although there was no legal assessment of ICN’s IP.
Governance

G.1 Effective governance

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

**Rationale:**

The ICN adopts a different premise with regard to effective governance. It states that “The nature of the PL Payments solutions obviates the need for participatory rule making by providers and/or users. Allowing such activity could destroy the inherent security of the system and nullify transaction insurance coverage.” If governance is necessary, it proposes that the Federal Reserve, the FDIC, and the OCC provide it. This level of governance does not currently occur for low-value payments. These three bodies could listen to suggestions or recommendations from provider and users for system enhancements. No governance disclosures or appeals process is described.

The criteria does call for effective participatory governance with the processes listed above and in G.1.

G.2 Inclusive governance

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

**Rationale:**

In general, it has been the approach of regulators and rules making bodies to establish rules/standards to minimize risk, determine liability of the participants and provide end users with recourse/reimbursement. The proposal indicates that regardless of potential regulator involvement in solution governance, that an independent governance group consisting of FIs and industry participants be created. The group should be diverse collection of bank representatives from large, regional and community banks and credit unions. This group will meet to discuss issues that pertain to rules or functionality required at the bank level and/or the end user level. In that case, it becomes a question for the ICN of whether it would be interested in reconsidering its stated stance and adopting an approach to both effective and inclusive governance that does not compromise its system and insurance but that meets the criteria’s requirements to some degree.
APPENDIX A: ASSESSMENT SUMMARY

✓ = QIAT Assessment
○ = Proposer Self-Assessment

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

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

<table>
<thead>
<tr>
<th>SAFETY AND SECURITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAFETY AND SECURITY (cont’d)</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>○ ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPEED (FAST)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.1: Fast approval</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>○ ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td>○ ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGAL</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1: Legal framework</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>○ ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>○ ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td>○</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td>○ ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1: Effective governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

✓ = QIAT Assessment  ○ = Proposer Self-Assessment
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

In general, the QIAT has done a good job laboring to comprehend, describe, and assess the InterComputer proposal against the effectiveness criteria. The questions posed to InterComputer were thoughtful and well deliberated. The conference call was very helpful and allowed us to ask questions about their questions. It is our opinion the process has been well defined by the Task Force and executed by the QIAT.

We also recognize the ratings are based upon what is “written in the proposal and Q&A response document.” Given that InterComputer’s solutions are not based on familiar 20th century bank technology practices, InterComputer’s proposal may have been more difficult to grasp than others. Our solutions are built on a deep, 21st century foundation of secure and efficient messaging, which obviates tediously complex rules and practices due to the ever-present settlement, technology, and human risks inherent in legacy systems.

Importantly, InterComputer has significant patent protection in real-time payments. We have disclosed many details about the core technology including our unique end-to-end eComprehensive Transaction Insurance, which covers all messages transferred on the network covering all participants and includes the face value of the payments. The industry has not yet learned how it works and why it is important to all parties involved in real-time TCP/IP Internet based transactions.

We disclose in the Q&A section of the proposal background and details of how it works and why it mitigates risk. Residual risk is so low the insurance coverage is extremely affordable. We recognize banks have certain cybercrime coverage in their data policies, but none cover all parties to a transaction crossing organizational, state, and international boundaries. Until bank payment technologists, their business counterparts, their legal department, top management and directors understand how the transaction insurance works, will they be unable to comprehend it. Dismissing it as not big enough to cover the daily volume of total money transferred in a day is an understandable but common error. Certain FDIC and OCC regulators are interested in the concept of Transaction Insurance as further strengthening a bank’s risk profile.

Also it is important to note that we have not included our Bank Service Level Agreement (SLA), which creates the legal finality of each payment in conjunction with the software. This legal agreement, which must be signed by all banks on the system, defines and memorializes the transfer of Commercial Bank Funds moving with the debit and credit clearing and settlement process. Not including this document in the formal proposal or Q&A document has cost us in effectiveness ratings in certain areas. But we will provide copies of the SLA under NDA as stated in the proposal and Q&A documents. IC’s Bank SLA had to be approved by Lloyd’s underwriters before they would include the face value of the payment in the policy. There has been substantial work and legal costs with a prominent New York law firm in laying out the legal framework and filling in the essential legal details.

So many people are now referring to our technology as “PrivateLine” as opposed to the IC IOS (InterComputer InterOperating System). These terms are becoming interchangeable and synonymous—and this fine with us. When reading the documentation, sometime both are used.

Our Comments on “Somewhat Effective” or “Not Effective” QIAT Ratings

Ubiquity
U.1 Accessibility – PrivateLine Payments (PL Pay) are available on all devices.
U.2 Usability:

The IC IOS or InterComputer InterOperating System strikes the necessary balance between security (closedness) and exposure (openness) to create accessibility and usability largely familiar to new users once initial registration and set-up is complete.

Predictability – One of the attributes of the IC IOS and the Trusted Settlement System is complete predictability accompanied by complete auditability for both payment data and contextual data. The IC IOS was designed according to a strict, risk-evaluated methodology and CMMI standards for quality control. A major part of the design and development process was flow charting all systems and sub-systems and have them validated by a team of Information Security, Software Security and Hardware Security experts. Predictability and repeatability are hallmarks of the IC IOS and InterComputer applications.

Efficiency

E.1 Enabling Competition – InterComputer makes its API (which includes the PrivateLine Control Bridge) available to FI’s, corporates, and developers. Both new and existing applications may be mapped to be used on ICN. At that point, all users of the software are provisioned by the same identity and authority X.509v3 digital certificates (including the AuthoriTree hierarchy) and receive all the same secure messaging and simplified identity and authority management benefits. Automatic policy enforcement on all messages, including all attributes of identity/authority, and all layers of protection, are all inherent in the ICN.

E.3 Implementation timeline – We do not disagree with the assessment. But with potential systemic risk of ubiquitous real-time payments it is essential that the right system is adopted and implemented correctly the first time. Any real-time payment system must have all nodes of equal strength. Anything less will result in systemic problems and specific institutional customer dissatisfaction and a delayed adoption curve. We did not describe hurdles we may expect. But our engineers are expert mappers. We have written and mapped interfaces for IBM 390 and 400 mainframes, client-server solutions and custom general ledger systems for large entities. We have found the most efficient implementations occur when an entity has a dedicated team to work with our team to define requirements per the bank IT topology, define a schedule, determine who on each team will perform the required tasks and communicate regularly by conference call. This is discussed in the Q&A. We have given ourselves a “Somewhat Effective” rating because total details, hurdles etc. cannot be credibly predicted until we go through the process. But we can state major mapping experiences can initially take six to eight weeks when both parties have a defined plan to move forward and keep on schedule and move into the testing phase. We have allotted six months of testing. Regulatory and other issues can be addressed simultaneously.

Ninety percent of ICN technology is common to all implementations. The other 10% is custom mapping to banks’ customer account systems. We recognize it will take 18 months to identify requirements, coordinate and achieve mapping from the bank’s customer account system to the IC IOS and Trusted Settlement. That period includes six months of testing for the largest banks. We believe regulatory approval (or at least concurrence) with any substantive volume of real-time payments is necessary, and we cannot know how long that process may take. The first major bank adoption will enable us to estimate the total implementation time with much greater accuracy. Some implementations will be easier than others.

E.7 Exceptions and investigations process – Apparently it was not clear enough in our proposal that the IC IOS has built-in features of system audit, forensic audit, and the ability to examine any one transaction or multiple transactions from the Control Bridge by authorized personnel at each bank. Because of the provisioning of organizations and users, not only is it known who initiated a
transaction, but who authorized it. Certain layers of software security are constantly operating on all messages sent and acknowledgements received to ensure messages have not been compromised in any way. Our proposal did not specify “who” at each institution is responsible for “what,” but the proposal does state that alerts are sent to all concerned parties of any suspicious transactions through the abuse/potential abuse system. This subsystem stops a suspicious payment instantly and sends the appropriate alerts to authorized employees. Potential Abuse rules annotate suspicious phenomena for investigation by authorized personnel to determine if an action or actions are anomalies or form a pattern of abuse. Authorized personnel are defined during FI set-up as a part of the installation and mapping requirements. If anything goes wrong in the system or if random sampling is required, the system is built for easy identification of the problem. Incident reports providing all relevant details to a transaction are immediately generated and available. Incident reporting which includes exceptions is a requirement in the SLA.

Safety and Security

Note: We did not include our SLA’s in the proposal, therefore, we do not fault the QIAT’s assessment rating. We rate our technology much higher in this category as we know the legal agreements which were approved by our underwriters. These agreements can be reviewed by any bank under NDA.

S.1 Unexpected application of a law or regulation – Our proposal indicates flexibility by the company and the software to adapt to changing laws or regulation. We did not define a step by step pathway to potential changes. But our methodology to making necessary changes is the same as designing and developing the software in the first place. Any such scenario involves designing and flow charting the changes and evaluating the impact of the changes to the system. Prototyping and coding the changes, Q&A testing, beta testing, and full roll-out.

S.3 Payment finality – As stated in the introduction to Appendix B, we did not disclose our SLAs in the proposal process. However, our patent includes technical details which support the legal framework which creates absolute legal finality where immediate funds availability occurs without legal recourse.

S.4 Settlement approach – The QIAT could follow the clearing and settlement process, but they could not distinguish the transfer of Commercial Funds concurrent with the debits and credits in the TSS system. In fairness to the QIAT, the establishment of official commercial funds is contained in the SLA which every bank on the system must agree to. Again, we will make the Bank SLA available under signed NDA.

S.5 Handling disputed payments – Our SLA creates absolute legal finality with each payment. IC participation in the FSTC Enterprise Architecture Committee in 2007 taught us that the legal departments at major banks were flooded with disputes concerning payments and check image clearing. Two enterprise architects at major banks indicated a reduction in bank legal costs through a legally binding process would be desirable. IC’s bank SLA can be modified and agreed upon as necessary. For example, if banks wish to provide added customer service, a rule for “payments made in error” can be established. (Despite the requirement to touch or click on two acceptance screens to preclude an inaccurate payee, it could happen.) In this case, a bank customer could call customer service, explain the error and the reason for it. The bank may require an ICN online form to be completed. If the bank determines the payment is errant, they can unwind and reverse the transaction. This example was not in our proposal. But the bank SLA is electronic, making it quick and easy to push out agreed upon changes to all banks and to be signed digitally with the authorized employees’ strong X.509v3 digital certificate.

S.6 Fraud information sharing – Since every participant on the network can digitally communicate with every other participant, necessary abuse and fraud rules can be described and applied universally. Nevertheless, any one institution has the ability to control who can see potential abuse or attempted
fraud that may occur within their organization. Technical fraud and abuse are prevented on the IC IOS as the system is that tight. But authorized individuals might attempt to engage in unauthorized activity, at which point alerts are sent to authorized personnel based upon the bank’s internal rules or the superset of rules for the ICN system. In this way, “disloyalty” fraud by insiders can be precluded through intelligent provisioning, where the number of authorized employees required to authorize any other employee is set.

S.8 Resiliency – The Solution has a mechanism and systems to ensure high levels of end-to-end availability and reliability under normal and stressed operating conditions. The proposal and Q&A state that the IC IOS is designed for scalability, limited only to available hardware and bandwidth. The proposal did not provide a throughput-per-second benchmark, which accounts for the “somewhat effective” rating. However, as the network grows, our benchmark is to build capacity 25% ahead of demand. With IC’s hosted/distributed architecture, adequate capacity and throughput will continually grow.

S.11 Participation requirements – ICN participation requirements are defined in the SLA, available with a signed NDA.

**Speed**

F.1 Fast Approval – This rating is low and results from not breaking down the payment cycle into a second by second count at each step. From other implementations and actual testing, we know that cycle times average 15 seconds. The approval within the validation system takes 5 seconds of this time as identities and authorities are cross validated. Ten seconds on average are required to move the messages through the system from end-to-end.

F.2 Fast clearing – the clearing (and settling) of debits and credits is almost instantaneous at each point.

F.2 Fast settlement – settling occurs (per the SLA) as each entry is cleared, but made official when all acknowledgement messages have been received end-to-end. The sending and acknowledging messages occur almost simultaneously.

**Governance**

G.1 – Effective governance & G.2 Inclusive Governance – Our proposal did not provide plans for a governing body to oversee and review possible rules, discuss potential problems, or propose new rules, e.g. abuse/fraud rules or features and desirable new features. In the Q&A, we did acknowledge that representatives across the body of stakeholders forming a committee or group should be established. Businesses don’t succeed when they do not define and deliver customer satisfaction. Understanding and agreement among regulators and government oversight committees are also essential. Such a group representing diverse stakeholders is necessary. We did state that independent representatives from large and medium size FI’s, Community Banks and Credit Unions should be represented. It would be wise to include representatives from the Fed, FDIC and OCC to observe, comment and recommend as needed.
INTERCOMPUTER CORP. PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

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

ICN Network is a real-time Internet protocol payment solution, closed loop, private network, supporting all cases including C2G, B2G, & G2G settles with Commercial banks, not central banks. Is difficult that this can be an end-to-end solution, with their main core participants being the Financial Institutions.

Super complicated solution.

The proposal is not in conformance with the requirements of a full solution proposal. The requirements were designed to ensure that McKinsey and Task Force time and resources are focused on end-to-end solution proposals that can be thoroughly and credibly assessed against the criteria. This proposal does not meet the requirements. Proposal has answered all sections of the template but in many cases the response does not provide information that would allow the QIAT to evaluate the proposal. The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a "detailed discussion of why the rating is justified and how the solution meets each criterion" (page 22 of template). It does not include specific information in Part C as to how or why the proposed solution meets each of the criteria. As a result, the QIAT is unable to evaluate the solution with the information provided. Altering the existing process defined to offer an opportunity for the proposer to include more explicit information in its submission to make the proposal “assessable” would be unfair to proposers who provided complete proposals before the submission deadline. A few of the reasons why the proposal did not meet the requirements are as follows: The solution did not address the unbanked. The solution has no governance framework. The solution has no deployment plan. The solution does not aggregate data across providers. The solution has no process to handle payment exceptions or disbursements.

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

A closed-loop system operating on a private network has both pluses and minuses. These are identified and (mostly) accurately assessed in the QIAT process. This accounts for the large cumulative number of "somewhat effective" and "not effective" ratings. There is one Effectiveness Criteria rating which I think should be lower. U2 - usability - the area for improvement section concluded that the enrollment process was a burdensome customer experience; this does not warrant an "effective rating."

The QIAT accurately assessed the proposal's technical strengths, but was fair in addressing the difficulties in the implementation and governance sections.

While I agree with most points of the assessment, I think the QIAT might have been a bit harsh in a few of the ratings. For example, rating "Not Effective" for Implementation Timeline based on the suggestion...
that a "strong regulatory impetus" may be necessary to gain fast adoption might be a bit harsh in that their statement is just speculation and is likely the reality for most solutions.

Very thorough QIAT review with deficiencies well noted. Solution has several areas that need to be addressed.

Rated fairly based on the information provided in the proposal; some important explanations were left out, and I agree the timeline was not realistic either.

Several key components within the effectiveness criteria associated with Legal were missing to be “effective.”

It is problematic to omit key pieces of the proposal, such as dispute handling, and request an NDA before viewing.

Proposal is lacking in areas of dispute resolution and governance, which was noted by QIAT.

Proposal does not demonstrate how the widespread adoption will be achieved. Fed is proposed as the regulator, which may or may not be a role they are willing to assume.

(1) Banks enroll customers, which could drive adoption (2) 18-30 month deployment (3) across mobile devices (4) 10-15 seconds (5) Limited to bank accounts so this helps with KYC, AMC, etc. (6) can set up a hierarchy of accounts to make payments (7) same user interface across payment channels (8) can initiate payment instructions with ACH and FED Wire (9) Can be connected to bank or treasury management/accounting systems.

Appears to have strong triple identity management characteristics. Lacks exception and dispute resolution process. Pushing disputes to the court systems to resolve issues will drive confidence in the overall solution. Use of jump drives—a security no-no!

Accessibility is rated too highly, as the proposal does not demonstrate how the solution allows users to reach any and all payees, nor how widespread adoption will be achieved – these are the core attributes of this ubiquity criteria. Detailed rules not available, so seems too highly rated. Settlement time appears to be rated too low based on description of how core system works.

While I agree with the overall assessment in general, it does seem overly negative toward areas where the proposal is stretching to cover. This is another technical proposal with some superior portions that seems to call for partnership in areas that are weaker. However, I do believe that some of the not effective ratings may have been overly stated because they are not linked to a direct proposal for the area. This is a difficult but continued theme on how to evaluate technical or targeted proposals in areas where they are not truly targeted.

Secure closed IP network, secured with digital certificates and 3-factor auth. 100% irrevocable push payments. Good APIs and value-add features for businesses. More end-user steps required for each transaction – cumbersome enrollment process. No pull payments. No governance. Timely

I believe that taken at face value the proposal was assessed properly. I struggle with how a new, closed-loop system that requires individual installations that will take 36 months for a community bank and a burdensome customer enrollment can be successful with ubiquitous implementation.

Overall the assessment is good, but I think they missed the mark on accessibility and usability. The solution requires any user to have a bank account (or requires would-be users to lobby their bank to offer the solution) so the underbanked are ignored. Also requires use of specific software on a smartphone (again, excludes anyone without a smartphone and assumes software is easy to deliver by mail). It is not effective for those two. Same with cross-border. Solution completely ignores rights of customers in consumer remittances (30 min window). It's barely somewhat effective for that. Granting the governance section "somewhat effective" is a little generous too, because they have a "wish list" for a governing body but nothing feasible in under a 3-5 year horizon.

The assessment is in line with my view of the effectiveness criteria. I am concerned about the amount of comments McKinsey makes regarding the need for a new solution to replace the current income issuers make on payments. I don't believe anywhere in the effectiveness criteria there is a requirement that the over-compensation for the completion of payments continue with a new system.

**TASK FORCE SOLUTION-ENRICHING COMMENTS**

**Ubiquity**

Without doubt, your approach could provide an extremely secure payments environment. But the perception left with me after review of your system makes me concerned that your solution appears to create an excessive amount of overhead. By this I mean, if it is difficult for a FI to implement (cross-bank agreements and user certificate maintenance), it will be difficult to obtain critical mass in adoption. With the added concern over the introduction of another settlement platform, FIs will opt for other solutions.

Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. Intercomputer relies on these organizations to cooperate with them in implementing the solution. To date, these companies have been unwilling to do this without significant compensation choosing instead to provide their own solutions. I would like to see a road map for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium-sized financial institutions. I would like to see a roadmap for how you will be able to work with core banking providers to roll out your system for community financial institutions.

The usability of the proposed solution could be enriched by streamlining the initial set-up required by both financial institutions and end-users. Additionally, the end-user’s experience could be enriched by modifying the requirement that terms and conditions be accepted by the payer each time a payment is initiated.
The burden placed on consumers to authenticate will slow down adoption. Provider should rethink process to eliminate steps.

I have some major concerns regarding ubiquity. The first issue is that from the proposal it seems that only banks can participate in the scheme. This ignores those who are unbanked or underbanked. The last paragraph of page 6 mentions banks only. On page 7 it talks about member banks. Then on the initiation page, page 13, it says enrolled bank or non-bank account provider. Is it only banks or can other FIs participate as well? I did not see specific standards listed in order to become a member of the scheme or to stay a member of the scheme.

The idea that end-users must sign up with CD or USB stick seems quite far-fetched. Not only will this be a barrier to entry because of the burden this will put upon end-users, this will be hard for those transient individuals in our society.

With participants having the ability to develop a wide variety of added-value services, describe how others in the system would know what information or formatting would be used with payments they receive from others.

U.1 Accessibility –Somewhat Effective, customers must be enrolled with a bank or credit union, banks must be participants for end-users to have access. Motivation for FIs cost and cyber crime reduction.

U.2 Usability—Somewhat Effective, users onboarding with the digital certificates is challenging. Based solely on “push” transactions and connections are based on end-users acting on a connection requested, similar to already similar technologies which create a hardship for the end-user and can unmotivated them from using the solution.

U.3 Predictability – Not Effective, disputes must be settled outside the payment system and in “court”—this approach immediately will drive away any potential participants.

U.5 Cross-border functionality –Not Effective, challenges with cross-border payments, and does not support any other transaction currencies only US dollar.

U.6 Applicability to Multiple Use Cases – Somewhat Effective, Challenges with cross-border use case.

The core of the solution seems very strong and targeted to the needs of a system. In general, this proposal could use more of a business orientation around the marketing for adoption and value proposition to banks. Very interesting proposal with security and privacy seemingly first in mind.

3 steps for end-user to complete – may feel cumbersome – wants it to be a mandate.

Customers have to have bank account – limits unbanked.

Web-based download not available for customers – will limit adoption.

Customer experience and end-user level can impede adoption, especially with unbanked having to rely on mailed USB or CD, strong regulatory impetus for broad adoption, end-users have to change banks if
their bank doesn’t offer – slows down and disrupts overall end-to-end user, overall, longer payment experience, motivation for FI adoption is ??, Implementation costs for FI will delay – and creation of correspondent banking network costs and time added.

I think ubiquity is the Achilles heel of this proposal. From a security aspect, sending software by mail or allowing download over a bank's network really enhance security, but if you have a widely disbursed customer base, especially if it is global, the expense and logistics of trying to manage sending items might be hard to make. If there's a way to make accessing the necessary software easier (you don't have to mail anything or force someone to come into a specific location), I think then it would have much better appear.

Limiting participants to requiring them to have a bank or credit union account restricts access to the system. Having a solution to address that would be beneficial. Entrance to the system seems very cumbersome, especially for special needs end-users. The more complicated the user experience, the less adoption success.

**Efficiency**

It was a little difficult to determine in your description how much could be automated via APIs in user setup vs. what required manual input. As a busy FI, we would not want to require a user to come into a bank branch for setup nor could we physically send a CD or USB key to safely install certificates. Also unclear to me was the impact to mobile-only users ...

The overall system could be enriched by modifying the overall user experience related to end-user authentication and transaction approval requirements which may assist in gaining wider adoption of the proposed solution.

Requirement to be at a participating FI and to re-register if accounts are switched creates a barrier for competition. Provider should consider changing system to allow for all stakeholders to participate and mobility of credentials.

Provide more information on how the solution can be supported by banks and their internal systems – not evident how the provided SDK works to allow for integration with existing systems.

E.1 Enables competition – Somewhat Effective, challenges as integration process is not described.

E.3 Implementation timeline – Not Effective, project timeline success is dependent on the substantial participation of a network of FIs, without a projected cost impact for an FI to participate.

E.7. Exceptions and investigations process – Not effective, a formal resolution or dispute process is not available, and there is no intention to develop a process unless is absolutely required by banks.
System is built, at least in part, upon user fees assessed by banks for processing paychecks. Banks save tremendous amounts of money by reducing the use of paper checks and cash, so it would seem that the reduction in check usage, as opposed to fees, would justify the practice.

2 applications for banks to install – additional costs and a lot of work.

No requirements to inform users about fees before payment occurs.

**Safety and Security**

Remove the use of jump drives as part of the solution—this is a major security issue.

The overall solution could be enriched by providing a clearer understanding of transactional insurance and the benefit of providing such insurance to the provider and end-user.

Further describe how to more easily support the security provisions – excellent high security, but seems cumbersome to enable SW individually for each end-user.

S.1 Risk Management – Not Effective, proposer states that risk can be mitigated through insurance coverage (protection), which would be difficult to entice participants to be part of this solution.

S.2 Payer Authorization & S.3 Payment finality – Somewhat Effective, payments are irrevocable and disputes can be addressed in a “court” system, this will be difficult for any participant to adopt.

S.4 Settlement Approach – Somewhat Effective, a trusted settlement account is required for FIs with transactions settling in 15 seconds, and can be map to the central bank settlement, adding 5 more seconds the transaction and configuring messaging.

S.5 Handling Disputes – Not Effective, no formal process is in place, their approach is to let the FIs dispute among themselves, and if needed form a committee to address these issues.

S.6. Fraud Information Sharing – Not Effective, no information is provided and no plan in place.

S.8 Resiliency – Not Effective, key critical items (e.g., required to have their own BCP and DRP for their nodes) are left to the participating FIs.

Maintenance of insurance policy to underwrite the activity only goes so far. If there is an issue and the insurance carrier ceases to cover the solution, it is unclear whether or not the solution is adequately secure in and of itself. Further, how much cost does this insurance add to the system? Could some of those costs, and the inconvenience associated with fraud, be eliminated with more robust security measures?

No process to handle dispute resolution /exceptions.

Need to strengthen dispute resolution capabilities/rules.
Handling disputed payments is a major concern, especially among FIs. Addressing this in the solution would be critical.

**Speed (Fast)**

The proposed 15-second authorization timeframe would eliminate the probability of the system being suitable for POS transactions which currently are authorized sub-one second.

F.1 Fast approval & F.2 Fast clearing – Somewhat Effective. Approval time is longer than the required 2 seconds, is 10-15 seconds.

F.4 Fast settlement among depository institutions & regulated non-bank account providers – Somewhat Effective, mapping the TSS system to the FIs’ Federal Reserve bank accounts “may have negative impact” on settlement due to operating hours.

Concerned about settlement speed and the perceived need to be part of the ICN to receive faster settlement.

**Legal**

The solution could be enhanced by providing additional information and the legal framework for the establishment of a new “correspondent bilateral system” and the ICNs Trusted Settlement System (TSS) application.

What steps will be taken to engage the Fed as regulator? (I.e., describe how this would be accomplished.) How will potential errors/disputes be handled? (Expand upon environment that may happen vs. anticipating that they will not exist.)

L.1 Legal framework – Somewhat Effective, the proposer’s addendum contradicts the “FPTF framework” and they stated they will provide details on a NDA.

**Governance**

I would have liked to see some suggested implementations for a governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution can be enriched by providing additional information around the governance model of the InterComputer Network (ICN).

The lack of thought on governance structure which is not inclusive of all stakeholders with voting rights leaves gaps in oversight.
I am concerned about the governance structure. There was no mention about end-user inclusion. It is important to have end-user inclusion in the process to present a unique perspective that FIs lack. Without inclusion not all important voices will be heard and not perspectives will be represented.

G.1 Effective governance & G.2 Inclusive governance - Somewhat Effective, if governance is required, it should be provided by government regulators such as the Federal Reserve, FDIC, and OCC.

This solution's proposal that the governance of the solution, which is a public utility, should be vested in the FED, FDIC, OCC, etc. is logical. Rather than leaving the solution open to the distortions that have arisen in today's payments system, it would be appropriate to ensure governance is handled by independent government agencies.

No governance framework.

Details need to be provided. Some statements seemed to be contradictory.

Would have appreciated more concrete ideas on the governance that would make this solution a great approach.
RESPONSES TO TASK FORCE ASSESSMENT COMMENTS

Introduction to Responses – January 23, 2017

We wish to thank the members of the FPTF who have taken the time to study our proposal and provide comments, both critical and constructive.

Most comments address three general themes:

1. Issues regarding the lack of governance details and the legal framework.
2. Issues regarding bank implementation, integration and registration of bank customers.
3. Issues pertaining to out-of-band mailing bank customers a pre-packaged CD, USB Key or MicroSD Card with the bank branded PrivateLine user interface.
   a. Asking bank customers who use only smartphones or tablets without access to an external drive come into a bank branch as previously mentioned.
   b. Getting the software to bank customers who may be located in hard to reach locations.

As a result, many of our answers are similar or the same. But we felt it best to address each comment irrespective of duplication. As noted in our responses, had we included in our proposal the Bank Service Level Agreements, many questions would have been answered. Including the SLA’s in the proposal would have likely resulted in higher assessment ratings in some areas.

These legal agreements which reflect specific processes, rules and requirements were developed at significant legal cost and are our intellectual property. Even though the system is 99.9999% effective, the SLAs had to be approved by our insurance underwriters before the eComprehensive transaction insurance against cybercrime, including the face value of money, was underwritten to cover residual risk. The end result of the proposal process includes the public release of the proposal and all documents considered in the QIAT Q&A, QIAT Assessment, Task Force comments and our responses. It would be unwise for us to put our SLAs into the public domain at this time.

The first section of our responses herein address each of the Concerns/Questions category of Assessment Comments in sequence format citing the segment, the concern or question followed by our response. The second section addresses the Solution Enhancing Comments in tabular format.

We also thank the Federal Reserve System, McKinsey, and the QIAT who tirelessly have reviewed and assessed our proposal, and for moving the Faster Payments upgrade forward on a level playing field. Last, we thank the Task Force steering committee, work group members and many other participants whom we have come to know and with whom we continue our association.
QUESTION/COMMENT – Other Stakeholders

1. A closed loop system operating on a private network has both pluses and minuses. These are identified and (mostly) accurately assessed in the QIAT process. This accounts for the large cumulative number of "somewhat effective" and "not effective" ratings. There is one effectiveness criteria ratings which I think should be lower. U2 - usability - the area for improvement section concluded that the enrollment process was a burdensome customer experience; this does not warrant an "effective rating".

IC ANSWER: “Burdensome” in this case is relative and subjective. The customer enrollment process is sufficiently involved to enable the benefits of insured security. Identifying oneself to one’s bank and installing an app on a smartphone are no more “burdensome” than opening a new account, and probably less so.

Enrollment Process for Banks
Page 41 of our proposal points out that once the IC IOS connection is mapped (including PrivateLine Control Bridge) to the FI, that customer enrollment can be performed on a branch-by-branch basis. Doing so reduces the registration function to approximately 3,000 to 15,000 bank accounts per branch depending on the size of the FI and the individual branches. In mapping the PrivateLine Control Bridge to the FI's operations centers or IT topology as they desire, bank branch employees are authorized to enroll customers with unique company identity digital certificates. The next step is registering organizations’ employees with unique identity and authority certificates, which enable the employee to transact with the bank. Authority certificates allow the organization and bank to control account access, set limits on transactions, or delegate authority to sign bank documents. Account opening or closing authority and extremely granular tasks are enabled by the settings generated in the digital authority certificate. Individual (consumer) customers are registered in the same way, branch by branch.

Enrollment Process for Bank Customers
The customer has no burden in the registration and set-up process except for a simple app installation routine. A bank- or InterComputer-generated CD or USB Key packaged and mailed out of band is easy to install. The pre-packaged CD or USB key does not contain any “secrets.” Once the customer installs the software, they are connected to their bank. All web cybercrime is obviated. They will view a customer agreement, which will contain the necessary legal language for absolute finality and other bank terms and fees. The bank customer can accept the agreement by use of their strong digital certificate’s “public key.” This signature is the strongest digital signature available. With all web cybercrime eliminated and an insured-secure messaging system, where is the burdensome experience?

Important points in connection with implementation and set-up:

1. Customer registration is done on a branch-by-branch basis, which makes the “elephant” easy to eat.

2. The PrivateLine Control Bridge has an "import" function. When mapped to the FI Customer Account software, the Control Bridge can import all existing customer information to minimize manual data entry.

3. Customers with mobile devices can go into any branch designated by the bank and download the app via a branch Wi-Fi system. This option is necessary because most mobile devices don’t have CD or USB drives. But nothing is required from bank employees to help customer’s set-up devices. The CD, USB Key, or branch Wi-Fi based download is a safe-process alternative to get the bank-branded PrivateLine user interface onto customer’s devices where a CD or USB is impractical. The wi-fi download will contain the mobile device and PC versions of PrivateLine. Platform coverage includes Windows, Mac, iPhone, and Android.
4. The IC closed-loop system grows from ICN users (FI’s, corporates, and individuals) registered by ICN and by developers using the API (Application Programming Interface) and associated SDK (Software Development Kit.) Page 2 of the QIAT response is quite detailed regarding the API of the IC IOS. The API SDK consists of the PrivateLine Control Bridge and specifications to enable authorized developers to code to it. Applications programmed to utilize the PrivateLine Control Bridge and run on ICN or InterComputer Network, all depend upon the identities of organizations, employees and authorities of who they are and what can they do within an application. The specifications define how to program to it and the documentation and testing required to obtain IC approval for entry and use of ICN.

QUESTION/COMMENT – Other Stakeholder

2. The QIAT accurately assessed the proposal's technical strengths, but was fair in addressing the difficulties in the implementation and governance sections.

IC ANSWER: Re: implementation, another questioner said, “I think the QIAT might have been a bit harsh in a few of the ratings. For example, rating "Not Effective" for Implementation Timeline based on the suggestion that a "strong regulatory impetus" may be necessary to gain fast adoption might be a bit harsh in that their statement is just speculation and is likely the reality for most solutions”.

With the potential systemic risk of ubiquitous real-time payments, it is essential that the right system is adopted and implemented correctly the first time. Any real-time payment system must have all nodes of equal strength. Anything less will result in systemic problems and specific institutional customer dissatisfaction and a delayed adoption curve.

Re: governance, our intent was to show maximum ability to conform to the eventual governing body's requirements. Addressing banking risk requires a role by the Fed/OCC/FDIC etc.

QUESTION/COMMENT – Medium Financial Institutions

3. While I agree with most points of the assessment, I think the QIAT might have been a bit harsh in a few of the ratings. For example, rating "Not Effective" for Implementation Timeline based on the suggestion that a "strong regulatory impetus" may be necessary to gain fast adoption might be a bit harsh in that their statement is just speculation and is likely the reality for most solutions . . .

IC ANSWER: We concur.

QUESTION/COMMENT – Medium Financial Institutions

4. Very thorough QIAT review with deficiencies well noted. Solution has several areas that need to be addressed.

IC ANSWER: We made the choice to limit our discussion of some areas, such as the unbanked. InterComputer has patented, proprietary technology that fully delivers all of our solution benefits to the unbanked, but we think it best that this discussion occurs after certain fundamental policies that are out of our control have been set. The comment that the solution does not address the “unbanked” is inaccurate. Among other places, the proposal addresses the unbanked on page 47 of the proposal.
QUESTION/COMMENT – Medium Financial Institutions

5. Rated fairly based on the information provided in the proposal, some important explanations were left out, and I agree the timeline was not realistic either.

IC ANSWER: Some explanations involve intellectual property that we are willing to disclose only under NDA. Re: timeline, we note that not all questioners share this view.

QUESTION/COMMENT – Medium Financial Institutions

6. Several key components within the effectiveness criteria associated with Legal were missing to be 'effective.'

IC ANSWER: Full legal explanations involve intellectual property that we are willing to disclose only under NDA. InterComputer did not include in its proposal the Bank SLA’s (Service Level Agreements) which memorializes funds transfer between banks as Commercial Funds, includes the language which establishes absolute legal finality, and provides the rules which apply to accomplish both. Both the Bank SLA and InterComputer Customer SLA were reviewed and approved by insurance underwriters to qualify for eComprehensive transaction insurance, including the value of money.

QUESTION/COMMENT – Consumer Interest Organizations

7. It is problematic to omit key pieces of the proposal, such as dispute handling, and request an NDA before viewing.

IC ANSWER: Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA.

QUESTION/COMMENT – Small Financial Institutions

8. Proposal is lacking in areas of dispute resolution and governance, which was noted by QIAT.

IC ANSWER: Our response with this concern is similar to the concern expressed in No. 7. Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA.

Regarding governance, we view governance as the role of the regulators. Our intent is to show maximum ability to conform to the eventual governing body’s requirements while offering innovative governance technologies. Potentially, existing rules and governance bodies can play a part in this role.

QUESTION/COMMENT – Other Stakeholders

9. Proposal does not demonstrate how the widespread adoption will be achieved. Fed is proposed as the regulator, which may or may not be a role they are willing to assume.
IC ANSWER: With potential systemic risk of ubiquitous real-time payments it is essential that the right system is adopted and implemented correctly the first time. Any real-time payment system must have all nodes of equal strength. Anything less will result in systemic problems and specific institutional customer dissatisfaction and a delayed adoption curve.

We fully anticipate that the Fed and other regulators will need to know, if not regulate, any widespread use of a real-time payment system.

QUESTION/COMMENT – Medium Financial Institutions

10. (1) Banks enroll customers-which could drive adoption (2) 18-30 month deployment (3) across mobile devices (4) 10-15 seconds (5) Limited to bank accounts so this helps with KYC, AMC, etc. (6) can set up a hierarchy of accounts to make payments (7) same user interface across payment channels (8) can initiate payment instructions with ACH and FED Wire (9) Can be connected to bank or treasury management/accounting systems.

IC ANSWER: We concur.

QUESTION/COMMENT – Other Stakeholders

11. Appears to have strong triple identity management characteristics. Lacks exception and dispute resolution process. Pushing disputes to the court systems to resolve issues will drive confidence in the overall solution. Use of jump drives - a security no-no!

IC ANSWER: Identity and Authentication characteristics are very strong.

Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver this function. Some explanations involve intellectual property that we are willing to disclose only under NDA. With respect to the single purpose “jump drives” and CD’s, they contain NO SECRETS merely bank-branded PrivateLine UI for installation on customer PC’s, networks and devices. Banks (or InterComputer) can prepare, package and issue USB Keys or CDs. The PrivateLine UI, once installed, connects the user to their bank over ICN for login and use.

QUESTION/COMMENT – Other Stakeholders

12. Accessibility is rated too highly, as the proposal does not demonstrate how the solution allows users to reach any and all payees, nor how widespread adoption will be achieved – these are the core attributes of this ubiquity criteria. Detailed rules not available, so seems too highly rated. Settlement time appears to be rated too lowly based on description of how core system works.

IC ANSWER: Part of InterComputer’s logo since 2003 is the word “connect.” Pages 45-46 under the heading “Integration Effort” of our proposal address connectivity/accessibility with the four, primary use-cases. But we should have provided more specific details how users access the payees and establish trusted connections. In many B2B scenarios, the accurate connection occurs during direct mapping between systems.
For small business systems, such as QB or Sage, we enable look-up directories for business partners to send “connect” requests (similar to Linked-in’s process). An employee authorization within the “authority certificate” must be enabled to submit a “connect” request and the “authority” to accept connection requests must be enabled on the receiver side. Only employees with these authorities can access the directory.

If companies choose, they do not have to show themselves in the directory. But a directory request to a particular company can be made anyway by authorized personnel. The “connect” request will still be sent to authorized employees for establishing accurate connections. Conversely, companies can terminate any connection at any time, for any reason.

For P2P based payments if a payer and payee have a personal transaction relationship, they can similarly connect. The personal directory is similar to the B2B in that people may choose not to be listed, but can be accessed if a friend, relative or other party knows their name, address and one other attribute. Internally, ICN validates the information and establishes an accurate, secure connection.

For P2B and B2P, the system works similarly but by a cell phone alias. The cell phone number, and digital certificate provisioned to that particular device establishes the connection. This includes point of sale transactions. The digital identity and authority certificates established by their own banks and validated on ICN ensure accurate connections.

As long as users have been registered by their banks, accessibility is automatically controlled. When necessary, human intervention to control connections is relatively seamless.

We concur with the settlement time assessment: with a 15-second average that INCLUDES clearing and settlement with legal finality, a high rating is well deserved.

**QUESTION/COMMENT – Non-Bank Providers**

13. While I agree with the overall assessment in general, it does seem overly negative toward areas where the proposal is stretching to cover. This is another technical proposal with some superior portions that seems to call for partnership in areas that are weaker. However, I do believe that some of the not effective ratings may have been overly stated because they are not linked to a direct proposal for the area. This is a difficult but continued theme on how to evaluate technical or targeted proposals in areas where they are not truly targeted.

**IC ANSWER:** It is also true that applying legacy criteria to an industry-changing solution can result in a misleading and ineffective evaluation.

**QUESTION/COMMENT – Other Stakeholders**


**IC ANSWER:** This view of the enrollment process is not shared by all reviewers. It basically consists of identifying oneself to one’s bank and installing an app on a PC or smartphone. To registration of users by
their banks is handled via the Control Bridge, which is designed for use by any non-technical bank employee authorized to do so.

Proffered flexibility for governance is not the same thing as "no governance". Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function.

The comment that the solution does not address the "unbanked" is inaccurate. Among other places, the proposal addresses the unbanked on page 47 of the proposal.

We agree that end-user steps may seem cumbersome, but in actuality, not necessarily so. For executing a payment, three clicks or three touches can occur very fast. The concept of one-touch is far overrated and far less secure. Even modern EMV card payments take a minimum of three interactions with the merchant terminal. Many require five or six interactions—and not in rapid sequence.

Although PrivateLine Payments does not allow debit pull payments, the proposal states it supports "pre-authorized push payments." A pre-authorized push payment is controlled by the payer, not the payee. After a conversation with the CFPB, we believe it is better to allow the payer to determine, set-up, and control automatic debits. In this way, should the payer decide to end the automatic debit, they can do so easily on their own. They don’t have to suffer additional automatic debits until another entity fulfills their instructions. Today, banks won’t stop automatic debits, but the organization such as a fitness center or a utility must take the steps to stop the automatic debit. Hence the new term, "pre-authorized push."

**QUESTION/COMMENT – Non-Bank Providers**

15. I believe that taken at face value the proposal was assessed properly. I struggle with how a new, closed loop system that requires individual installations that will take 36 months for a community bank and a burdensome customer enrollment can be successful with ubiquitous implementation.

**IC ANSWER:** This view of the enrollment process is not shared by all reviewers. It basically consists of identifying oneself to one’s bank and installing an app on a PC or smartphone. The registration of users by their banks is handled via the Control Bridge, which is designed for use by any non-technical bank employee authorized to do so.

We have acknowledged the importance of the regulator’s role in advancing adoption and implementation. With the potential systemic risk of ubiquitous real-time payments, it is essential that the right system is adopted and implemented correctly the first time. Any real-time payment system must have all nodes of equal strength. Anything less will result in systemic problems, specific institutional customer dissatisfaction, and a delayed adoption curve.

Although ICN is a closed-loop solution, it is the only closed loop network which obviates all web cybercrime, with multiple layers of protection automatically enforcing all messages with all protections, all the time. There is no human error. ICN has an API and SDK which enable banks, corporates and other third-party providers access the network and enlarge it.

Because of the layers of protection and obviating web cybercrime, ICN carries unique eComprehensive transaction insurance which covers all messages end-to-end including the value of money. Limits grow with transactional activity. No other closed-loop network offers this level of security, functionality and providing insurance protection. These features set ICN apart.
QUESTION/COMMENT – Non-Bank Providers

16. ICN Network is a real-time Internet protocol payment solution, closed loop, private network, supporting all cases including C2G, B2G, & G2G settles with Commercial banks, not central banks. Is difficult that this can be an end-to-end solution, with their main core participants being the Financial Institutions.

IC RESPONSE: The statement, “it’s difficult that this be an end-to-end solution, with their main core participants being the FIs” is inaccurate. InterComputer offers any bank that will partner with us:

1. A non-web, insured-secure connection to all their customers, organizations and consumers.
   a. A bank-branded PrivateLine connection protects their customers, stockholders, executives and directors from web-based cybercrime.
   b. The bank branded PrivateLine user interface can leverage their current PHP and HTML programming, while web URLs are not used. Addressing is achieved as each bank customer is registered by the bank, and then connected to their desired payees.
   c. Banks can add functionality to their offerings not available with web-based online banking.
   d. Banks can generate significant new revenue with their efforts.
   e. Bank can save all costs associated with web security, which is an enormous savings in money and personnel.

2. It is not a large leap to recognize that once bank customers are connected securely to their banks, they can connect to each other for all use cases of payment transactions with added functionality such as PL tMail, PL tChat, Contextual Chat (document-to-document), remittances interoperating between systems, either subject to human control or fully automatic.

3. Our proposal does have an alternate implementation consistent with our patented IP to move money in Central Bank funds. Please refer to the QIAT Q & A document, page 11.

The fact that our solution delivers insured functionality and legal finality from end-to-end is fully documented throughout our proposal.

QUESTION/COMMENT – Medium Financial Institutions

17. Overall the assessment is good but I think they missed the mark on accessibility and usability. The solution requires any user to have a bank account (or requires would be users to lobby their bank to offer the solution) so the underbanked are ignored. Also requires use of specific software on a smartphone (again, excludes anyone without a smartphone and assumes software is easy to deliver by mail). It is not effective for those two. Same with cross border. Solution completely ignores rights of customers in consumer remittances (30 min window). It's barely somewhat effective for that. Granting the governance section “somewhat effective” is a little generous too because they have a "wish list" for a governing body but nothing feasible in under a 3-5 year horizon.

IC ANSWER: We made the choice to limit our discussion of some areas, such as the unbanked. InterComputer has patented, proprietary technology that fully delivers solution benefits to the unbanked, as noted on page 47 of our proposal. We think it best that a full discussion occurs after certain fundamental policies that are out of our control have been set. The comment that the solution does not address the “unbanked” is inaccurate. Among other places, the proposal addresses the unbanked on page 47 of the proposal.
The “30-minute window of cancellation” for international remittances was created by the Dodd-Frank amendments regarding remittance transfers are contained in subpart B to Regulation E and applies to cross-border payments made by any solution the task force eventually recommends or adopts.

Proffered flexibility for governance is not the same thing as “no governance”. Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Any two banks cannot implement PrivateLine and sign the Bank SLA (digitally signed and updated on the system). The rules contained in it are fully backed by eComprehensive transaction insurance.

**QUESTION/COMMENT – Other Stakeholders**

18. The proposal is not in conformance with the requirements of a full solution proposal.

The requirements were designed to ensure that McKinsey and Task Force time and resources are focused on end-to-end solution proposals that can be thoroughly and credibly assessed against the criteria.

This proposal does not meet the requirements.

Proposal has answered all sections of the template but in many cases the response does not provide information that would allow the QIAT to evaluate the proposal.

The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a “detailed discussion of why the rating is justified and how the solution meets each criterion” (page 22 of template). It does not include specific information in Part C as to how or why the proposed solution meets each of the criteria. As a result, the QIAT is unable to evaluate the solution with the information provided.

Altering the existing process defined to offer an opportunity for the proposer to include more explicit information in its submission to make the proposal “assessable” would be unfair to proposers who provided complete proposals before the submission deadline.

A few of the reasons why the proposal did not meet the requirements are as follows:

- The solution did not address the unbanked.
- The solution has no governance framework.
- The solution has no deployment plan.
- The solution does not aggregate data across providers.
- The solution has no process to handle payment exceptions or disbursements.

**IC ANSWER:** We made the choice to limit our discussion of some areas, such as the unbanked. InterComputer has patented, proprietary technology that delivers solution benefits to the unbanked, but we think it best that this discussion occurs after certain fundamental policies that are out of our control have been set. The comment that the solution does not address the “unbanked” is inaccurate. Among other places, our proposal addresses the unbanked on page 47.

With Governance, our intent was to show maximum ability to conform to the eventual governing body’s requirements while offering innovative governance technologies. Addressing banking risk requires a role by the Fed/OCC/FDIC etc.

Dispute handling, as viewed in the traditional sense, is obviated by our solution which is back by eComprehensive insurance. There are no fraudulently initiated payments, inaccurate routing of payments
etc. After “touching” or “clicking” one time, the payer has two opportunities to stop the payment. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA.

Although some might not like our implementation plan and timeline, we do have a plan and it is located in the implementation section of the proposal.

**QUESTION/COMMENT** – Business End Users

19. The assessment is in line with my view of the effectiveness criteria. I am concerned about the amount of comments McKinsey makes regarding the need for a new solution to replace the current income issuers make on payments. I don’t believe anywhere in the effectiveness criteria there is a requirement that the over compensation for the completion of payments continue with a new system.

**IC ANSWER:** Our view is that banks must be incentivized to perform their role in the adoption of whatever solution results from this task force. The solution may result in a marked reduction in bank fees for NSF incidents and Fedwire payments. But the value add from our solution far exceeds its cost to end users while providing banks with a healthy financial incentive.
### INTERCOMPANY RESPONSES TO SOLUTION ENRICHING CONCERNS AND QUESTIONS

<table>
<thead>
<tr>
<th>SEGMENT</th>
<th>CRITERIA</th>
<th>CONCERN/QUESTION</th>
<th>ANSWER/COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Stakeholders</td>
<td>Safety &amp; Security</td>
<td>Remove the use of jump drives as part of the solution - this is a major security issue</td>
<td>In our case, “jump drives” contain NO SECRETS. Banks (or InterComputer) can prepare, package and issue jump drives or CDs or micro-SD cards containing the client app code. The bank-branded PrivateLine will only function over an ICN connection, insuring security for any secrets.</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Ubiquity</td>
<td>Without doubt, your approach could provide an extremely secure payments environment. But the perception left with me after review of your system makes me concerned that your solution appears to create an excessive amount of overhead. By this I mean, if it is difficult for a FI to implement (cross bank agreements and user certificate maintenance), it will be difficult to obtain critical mass in adoption. With the added concern over the introduction of another settlement platform, FIs will opt for other solutions.</td>
<td>This view of the enrollment process is not shared by all reviewers. It basically consists of identifying oneself to one’s bank and installing an app on a PC or smartphone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The registration of users by their banks is handled via the Control Bridge, which is designed for use by any non-technical bank employee authorized to do so.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Banks sign only one agreement, and all participant banks sign the same agreement, which may be revised and updated electronically for low overhead.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>There is set-up involved with any solution. These new procedures may seem or be cumbersome, but not overtly so. It is better to provide bank customers, shareholders, executives and directors a system free from cybercrime backed by unique insurance designed for the 21st century.</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Efficiency</td>
<td>It was a little difficult to determine in your description how much could be automated via APIs in user setup vs what required manual input. As a busy FI, we would not want to require a user to come into a bank branch for setup nor could we physically send a CD or USB key to safely install certificates. Also unclear to me was the impact to mobile-only users ...</td>
<td>The API and automation tools for bank set-up depend upon the requirements determined by banks and IC developers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Our proposal only requires a user to go to a bank branch to download the app unless they only have a smartphone without a micro SD slot, or they choose to. In this case they download the PrivateLine UI app over the branch’s dedicated Wi-Fi. PC Users may load the app from a CD or USB key supplied either by the bank or by InterComputer. USB keys/CDs contain NO SECRETS merely the bank branded PrivateLine UI. Impact to mobile users? Peace of mind regarding privacy and cybercrime plus new functionality FI’s wish to add over the secure connections.</td>
</tr>
<tr>
<td>Non-Bank Providers</td>
<td>Ubiquity</td>
<td>Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. InterComputer relies on these organizations to cooperate with them in implementing the solution. To date, these companies have been unwilling to do this without significant compensation choosing instead to provide their own solutions. I would like to see a roadmap for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium sized financial institutions. I would like to see a roadmap for how you will be able to work with core banking providers to roll out your system for community financial institutions.</td>
<td>None of the providers to which you refer has an end-to-end insured secure solution with full legal finality to offer anyone. While not essential to our roll out, we value their cooperation and can offer strong incentive for it. If needed, community banks and credit unions can ask their software providers to enable a PrivateLine connection for their institution. If FISERV, FIS, Jack Henry and others provide documented API’s IC has the expertise to map to those systems. But it is logical that these entities may need to help their bank customers.</td>
</tr>
<tr>
<td>Non-Bank Providers</td>
<td>Governance</td>
<td>I would have liked to see some suggested implementations for a governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments systems.</td>
<td>Addressing banking risk and associated governing policies will require a Fed/OCC/FDIC or other existing rules and governance bodies to perform this role.</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Ubiquity</td>
<td>The usability of the proposed solution could be enriched by streamlining the initial set-up required by both financial institutions and end-users. Additionally, the end-users experience could be enriched by modifying the requirement that terms and conditions be accepted by the payer each time a payment is initiated.</td>
<td>Streamlining can be addressed at the time of initial set-up as IC developers meet with assigned FI personnel to define installation requirements and procedures. Three or more touches for end-users should not be a hindrance. In our case, touches or clicks are easier than interacting with EMV PoS readers. REG E requires legal disclaimers if device is considered “an access device” under the law. Two legal confirmations with appropriate disclosure language, one from the customer record and one from the bank record, are required to establish legal finality if the Fed should classify any payment device, such as a smartphone as an “access device.”</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Efficiency</td>
<td>The overall system could be enriched by modifying the overall user experience related to end-user authentication and transaction approval requirements which may assist in gaining wider adoption of the proposed solution.</td>
<td>Three to five interactions (in our case, touches or clicks) are necessary for EMV. The touches or clicks are fast and simple. REG E requires legal disclaimers if device is considered “an access device” under the law. Two legal confirmations, one</td>
</tr>
</tbody>
</table>
from the customer record and one from the bank record, are required to establish legal finality.

<table>
<thead>
<tr>
<th>Medium Financial Institutions</th>
<th>Safety &amp; Security</th>
<th>The overall solution could be enriched by providing a clearer understanding of transactional insurance and the benefit of providing such insurance to the provider and end-user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium Financial Institutions</td>
<td>Legal</td>
<td>The solution could be enhanced by providing additional information and the legal framework for the establishment of a new 'correspondent bilateral system' and the ICNs Trusted Settlement System (TSS) application.</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Governance</td>
<td>The solution code be enriched by providing additional information around the governance model of the InterComputer Network (ICN).</td>
</tr>
<tr>
<td>Non-Bank Providers</td>
<td>Ubiquity</td>
<td>Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. InterComputer relies on these organizations to cooperate with them in implementing the solution. To date, these companies have been unwilling to do this without significant compensation choosing instead to provide their own solutions. I would like to see a roadmap for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium sized financial institutions. I would like to see a roadmap for how you will be able to work with core banking providers to roll out your system for community financial institutions.</td>
</tr>
<tr>
<td>Non-Bank Providers</td>
<td>Governance</td>
<td>I would have liked to see some suggested implementations for a governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments systems.</td>
</tr>
</tbody>
</table>

Transaction insurance is mentioned and discussed in more than 20 places throughout our proposal. Specifically, it is detailed in pages 16-22 of the QIAT Q&A document. It covers all parties to a covered transaction against loss due to system malfunction or cybercrime of any kind. This coverage includes the face value of the transaction and lost business.

Full legal explanations involve intellectual property in our Bank SLA’s that we are willing to disclose only under NDA. The Bank SLA’s have been approved by insurance underwriters.

Re: governance, our intent was to show maximum ability to conform to the eventual governing body's requirements while offering innovative governance technologies. Addressing banking risk requires a role by the Fed/OCC/FDIC etc.

None of the providers to which you refer has an insured secure solution with full legal finality to offer anyone. While not essential to our roll out, we value their cooperation and can offer strong incentive for it.

Re: governance, our intent was to show maximum ability to conform to the eventual governing body's requirements while offering innovative governance technologies. Addressing banking risk requires a role by the Fed/OCC/FDIC etc.
<p>| Medium Financial Institutions | Ubiquity | The usability of the proposed solution could be enriched by streamlining the initial set-up required by both financial institutions and end-users. Additionally, the end-users experience could be enriched by modifying the requirement that terms and conditions be accepted by the payer each time a payment is initiated. | Three or more touches (in our case, clicks) are necessary for EMV. Ours are even easier than the EMV approach. REG E requires legal disclaimers if device is considered “an access device” under the law. Two legal confirmations, one from the customer record and one from the bank record, are required to establish legal finality. |
| Medium Financial Institutions | Efficiency | The overall system could be enriched by modifying the overall user experience related to end-user authentication and transaction approval requirements which may assist in gaining wider adoption of the proposed solution. | The ability to login and authenticate at a 99.9999% reliability rate require certain actions. |
| Medium Financial Institutions | Safety &amp; Security | The overall solution could be enriched by providing a clearer understanding of transactional insurance and the benefit of providing such insurance to the provider and end-user. | Transaction insurance is mentioned and discussed in more than 20 places throughout our proposal. Specifically, pages 16-22 of the QIAT Q&amp;A document provides specific detail. It covers all parties to a covered transaction against loss due to system malfunction or cybercrime of any kind. This coverage includes the face value of the transaction. |
| Medium Financial Institutions | Legal | The solution could be enhanced by providing additional information and the legal framework for the establishment of a new 'correspondent bilateral system' and the ICNs Trusted Settlement System (TSS) application. | The Bank SLA’s contain the legalese and rules which have been approved by underwriters. They are valuable intellectual property that we are willing to disclose only under NDA. |
| Business End Users | Ubiquity | The burden placed on consumers to authenticate will slow down adoption. Provider should rethink process to eliminate steps. | Single transaction authentication is fully automated. If by “authentication” you mean registration, “burdensome” is relative. The customer enrollment process is sufficiently involved to enable the benefits of insured security. Identifying oneself to one’s bank and installing an app on a smartphone or PC are no more “burdensome” than opening a new bank account, and probably less so. |
| Business End Users | Efficiency | Requirement to be at a participating FI and to re-register if accounts are switched creates a barrier for competition. Provider should consider change system to allow for all stakeholders to participate and mobility of credentials. | Usage of the system involves each user having two certificates: one establishing identity, the other establishing authority limits. The identity certificate is theoretically mobile, the authority certificate is not because each bank has its own policies to enforce. A consumer must visit a bank branch to |</p>
<table>
<thead>
<tr>
<th><strong>Business End Users</strong></th>
<th><strong>Speed</strong></th>
<th>The proposed 15 second authorization timeframe would eliminate the probability of the system being suitable for POS transactions which currently are authorized sub-one second.</th>
<th>The 15-second period is not for authorization only; in that time, the entire transaction is executed, cleared, and settled with legal finality and insured security. The feasibility request and acknowledgement (approval) takes 2 seconds, on average, with the remainder of the end-to-end cycle 13 additional seconds, on average.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business End Users</strong></td>
<td><strong>Governance</strong></td>
<td>The lack of a thought our governance structure which is not inclusive of all stakeholders with voting rights leaves gaps in oversight.</td>
<td>We view governance as the role of the regulators. Addressing banking risk requires a role by the Fed/OCC/FDIC etc. Our intent was to show maximum ability to conform to the eventual governing body’s requirements while offering innovative governance technologies. However, we have reviewed the suggestion you make and continuing efforts to provide this eventuality.</td>
</tr>
<tr>
<td><strong>Government End User</strong></td>
<td><strong>Ubiquity</strong></td>
<td>I have some major concerns regarding ubiquity. The first issue is that from the proposal it seems that only banks can participate in the scheme. This ignores those who are unbanked or underbanked. The last paragraph of page 6 mentions banks only. On page 7 it talks about member banks. Then on the initiation page, page 13, it says enrolled bank or non-bank account provider. Is it only banks or can other FIs participate as well? I did not see specific standards listed in order to become a member of the scheme or to stay a member of the scheme. The idea that end users must sign up with CD or USB stick seems quite far-fetched. Not only will this be a barrier to entry because of the burden this will put upon end users, this will be hard for those transient individuals in our society.</td>
<td>Page 47 of our proposal does address the unbanked from a smartphone perspective. We have used the word, “bank” generically throughout our proposal to mean any legally authorized depository institution (bank, commercial bank, community bank, savings and loan, credit union, etc.). We also anticipate the possibility of third parties such as authorized money transmitters like PayPal, Western Union, etc. or non-bank providers like VISA, MasterCard, American Express desiring to use our solution. Any FI who is a member of the Federal Reserve System qualifies. Sending non-web apps through the web is dangerous. A one-time out-of-band delivery for initial installation is not much to require for freedom from cybercrime. No unlike registering for Compuserve, AOL, Prodigy or others in times past. The benefits far outweigh a one-time process.</td>
</tr>
<tr>
<td><strong>Government End User</strong></td>
<td><strong>Governance</strong></td>
<td>I am concerned about the governance structure. There was no mention about end user inclusion. It is important to have end user inclusion in the process to present a unique perspective that FIs lack. Without inclusion not all important voices</td>
<td>We view governance as the role of the regulators. But your suggestion is well taken. Addressing banking risk requires a role by the Fed/OCC/FDIC etc. Our intent was to show maximum ability to conform to the eventual governing body’s requirements while offering innovative governance technologies. The “inclusion” you suggest will be considered.</td>
</tr>
<tr>
<td>Other Stakeholders</td>
<td>Ubiquity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>will be heard and not perspectives will be represented.</td>
<td>Payment formats are automatically standardized by our solution. Applications other than payments must adhere to our SDK/API, which will be legally governed by the terms of the license. In many cases, our mapping engineers may need to translate formats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>With participants having the ability to develop a wide variety of added value services, describe how others in the system would know what information or formatting would be used with payments they receive from others</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Stakeholders</td>
<td>Efficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide more information on how the solution can be supported by banks and their internal systems – not evident how the provided SDK works to allow for integration with existing systems</td>
<td>The SDK/API will be available to legal licensees of our solution. Its usage will be governed by the license terms. It allows internal applications to be developed and deployed on ICN to perform the work required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Stakeholders</td>
<td>Safety &amp; Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Further describe how to more easily support the security provisions – excellent high security, but seems cumbersome to enable SW individually for each end user.</td>
<td>The customer enrollment process is sufficiently involved to enable the benefits of insured security. Identifying oneself to one’s bank and installing an app on a smartphone or PC are no more “burdensome” than opening a new bank account, and probably less so. It’s a one-time event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Stakeholders</td>
<td>Legal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What steps will be taken to engage the Fed as regulator? (i.e., describe how this would be accomplished). How will potential errors/dispute be handled? (Expand upon environment that may happen vs. anticipating that they will not exist).</td>
<td>We assume the Fed will determine its role as a regulator in real-time payment administration. We are ready to engage the Fed on this topic now. Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Bank Providers</td>
<td>Ubiquity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UBIQUITY U.1 Accessibility –Somewhat Effective, customers must be enrolled with a bank or credit union, banks must be participants for end-users to have access. Motivation for FI’s cost and cybercrime reduction. U.2 Usability-Somewhat Effective, users on boarding with the digital certificate is challenging. Based soled on ‘push’ transactions and connections are based on end-users acting</td>
<td>The customer enrollment process is sufficiently involved to enable the benefits of insured security. Identifying oneself to one’s bank and installing an app on a smartphone or PC are no more “burdensome” than opening a new bank account, and probably less so. Usage of the system involves each user having two certificates: one establishing identity, the other establishing authority limits. The identity certificate is theoretically mobile, the authority certificate is not because each bank has its own policies to enforce. A consumer must visit a bank branch to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Bank Providers</td>
<td>Efficiency</td>
<td>EFFICIENCY</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E.1 Enables competition – Somewhat Effective, challenges as integration process is not described.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E.3 Implementation timeline – Not Effective, project timeline success is dependent on the substantial participation of a network of FIs, without a projected cost impact for an FI to participate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E.7. Exceptions and investigations process – Not effective, a formal resolution or dispute process is not available, and there is no intention to develop a process unless is absolutely require by banks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Bank Providers</th>
<th>Safety &amp; Security</th>
<th>SAFETY AND SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S.1 Risk Management – Not Effective, proposer states that risk can be mitigated through insurance coverage (protection), which would be difficult to entice participants to be part of this solution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.2 Payer Authorization &amp; S.3 Payment finality – Somewhat Effective, payments are irrevocable and disputes can be addressed in a “court”</td>
<td></td>
</tr>
</tbody>
</table>

| U.3 Predictability – Not Effective, disputes must be settle outside the payment system and in “court”—which this approach immediately will drive away any potential participants. |
| U.5 Cross-border functionality – Not Effective, challenges with cross-border payments, and does not support any other transaction currencies only US dollar. |
| U.6 Applicability to Multiple Use Cases – Somewhat Effective, Challenges with cross-border use case |

| establish a new account at that bank, and there is no reason new certificates cannot be issued at that time. |
| Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA. |

| The SDK/API will be available to legal licensees of our solution. Its usage will be governed by the license terms. |
| Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA. |

| Our unique transaction insurance does not merely mitigate risk: it eliminates it. Lloyds would never have underwritten our solution unless all but a tiny, residual risk were eliminated by the solution itself. After more than a year of rigorous evaluation and scrutiny, Lloyds knew that was the case and made their underwriting decision. This insurance is now also available from U.S. underwriters for sufficiently secure systems. |
system, this will be difficult for any participant to adopt.  
S.4 Settlement Approach – Somewhat Effective, a trusted settlement account is required for by FI’s with transaction settling in 15 seconds, and can be map to the central bank settlement, adding 5 more second the transaction and configuring messaging.  
S.5 Handling Disputes – Not Effective, no formal process is in place, their approach is to let the FI’s dispute among themselves, and if needed form a committee to address these issues.  
S.6 Fraud Information Sharing – Not Effective, no information is provided and no plan in place.  
S.8 Resiliency – Not Effective, key critical items (e.g., required to have their own BCP and DRP for their nodes) are left to the participating FIs

<table>
<thead>
<tr>
<th>Non-Bank Providers</th>
<th>Speed</th>
<th>SPEED (FAST)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F.1 Fast approval &amp; F.2 Fast clearing – Somewhat Effective approval time is longer than the require 2 seconds, is 10-15 seconds.</td>
<td>F.1 Fast approval &amp; F.2 Fast clearing – Somewhat Effective approval time is longer than the require 2 seconds, is 10-15 seconds.</td>
</tr>
<tr>
<td></td>
<td>F.4 Fast settlement among depository institutions &amp; regulated non-bank account providers – Somewhat Effective, mapping the TSS system to the FI’s Federal Reserve bank accounts “may have negative impact” on settlement due to operating hours.</td>
<td>F.4 Fast settlement among depository institutions &amp; regulated non-bank account providers – Somewhat Effective, mapping the TSS system to the FI’s Federal Reserve bank accounts “may have negative impact” on settlement due to operating hours.</td>
</tr>
</tbody>
</table>

Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. The legal framework underpinning the solution guarantees legal finality for transactions. A transactor must confirm the transaction at least twice before it is executed.

<table>
<thead>
<tr>
<th>Non-Bank Providers</th>
<th>Legal</th>
<th>LEGAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L.1 Legal framework – Somewhat Effective, the proposer’s addendum contradicts the “FPTF framework” and they stated they will provide details on a NDA.</td>
<td>L.1 Legal framework – Somewhat Effective, the proposer’s addendum contradicts the “FPTF framework” and they stated they will provide details on a NDA.</td>
</tr>
</tbody>
</table>

The 15-second average INCLUDES clearing and settlement with legal finality, not just “approval”.

<table>
<thead>
<tr>
<th>Non-Bank Providers</th>
<th>Governance</th>
<th>GOVERNANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>G.1 Effective governance- &amp; G.2 — Inclusive governance - Somewhat Effective, if governance is required, it should be provided by government</td>
<td>G.1 Effective governance- &amp; G.2 — Inclusive governance - Somewhat Effective, if governance is required, it should be provided by government</td>
</tr>
</tbody>
</table>

Full legal explanations involve intellectual property that we are willing to disclose only under NDA.

Governance should include a formal mechanism for the input of the governed to the process of answering questions and deciding issues.
<table>
<thead>
<tr>
<th>Non-Bank Providers</th>
<th>Ubiquity</th>
<th>The core of the solution seems very strong and targeted to the needs of a system. In general, this proposal could use more of a business orientation around the marketing for adoption and value proposition to banks. Very interesting proposal with security and privacy seemingly first in mind.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business End Users</td>
<td>Efficiency</td>
<td>System is built, at least in part, upon user fees assessed by banks for processing paychecks. Banks save tremendous amounts of money by reducing the use of paper checks and cash, so it would seem that the reduction in check usage, as opposed to fees, would justify the practice.</td>
</tr>
<tr>
<td>Business End Users</td>
<td>Safety &amp; Security</td>
<td>Maintenance of insurance policy to underwrite the activity only goes so far. If there is an issue and the insurance carrier ceases to cover the solution, it is unclear whether or not the solution is adequately secure in and of itself. Further, how much cost does this insurance add to the system? Could some of those costs, and the inconvenience associated with fraud, be eliminated with more robust security measures?</td>
</tr>
<tr>
<td>Business End Users</td>
<td>Governance</td>
<td>This solution's proposal that the governance of the solution, which is a public utility, should be vested in the FED, FDIC, OCC, etc. is logical. Rather than leaving the solution open to the distortions that have arisen in today's payments system, it would be appropriate to ensure governance is handled by independent government agencies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With potential systemic risk of ubiquitous real-time payments <strong>it is essential that the right system is adopted and implemented correctly the first time.</strong> Any real-time payment system must have all nodes of equal strength. Anything less will result in systemic problems and specific institutional customer dissatisfaction and a delayed adoption curve.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We anticipate that users will view the real-time, insured secure nature of our solution as value far in excess of the fees banks may charge. Banks need incentive to adopt the solution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The cost of our unique transaction insurance, at volume, is pennies per transaction. The underwriter would never insure the system unless doing so were profitable. The initial underwriters spent more than a year analyzing and testing the security of our system before making the decision to underwrite it. Our solution is the ONLY underwritten solution in the world, which says something strongly: for this application, we are as good as it gets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We view governance as the role of the regulators. Our intent is to show maximum ability to conform to the eventual governing body's requirements while offering innovative governance technologies.</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Ubiquity</td>
<td>3 Steps for end user to complete – may feel cumbersome – wants it to be a mandate customers have to have bank account – limits unbanked web based download not available for customers - will limit adoption Customer experience and end user level can impede adoption, especially with unbanked having to rely on mailed USB or CD, strong regulatory impetus for broad adoption, end users have to change banks if their bank doesn’t offer – slows down and disrupts overall end to end user, overall, longer payment experience, motivation for FI adoption is ??, Implementation costs for FI will delay – and creation of correspondent banking network costs and time added</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Efficiency</td>
<td>2 applications for banks to install – additional costs and a lot of work no requirements to inform users about fees before payment occurs</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Safety &amp; Security</td>
<td>No process to handle dispute resolution /exceptions</td>
</tr>
<tr>
<td>Medium Financial Institutions</td>
<td>Governance</td>
<td>no governance framework</td>
</tr>
</tbody>
</table>
| Other Stakeholders | Ubiquity | UBIQUITY  
U.1 Accessibility – Somewhat Effective, customers must be enrolled with a bank or credit union, banks must be participants for end-users to have access. Motivation for FI’s cost and cybercrime reduction.  
U.2 Usability-Somewhat Effective, users on boarding with the digital certificates is challenging. Based solely on ‘push’ transactions and connections are based on end-users acting on a connection requested, similar to already similar technologies which create a hardship for the end-user and can unmotivate them from using the solution.  
U.3 Predictability – Not Effective, disputes must be settle outside the payment system and in “court”—which this approach immediately will drive away any potential participants.  
U.5 Cross-border functionality – Not Effective, challenges with cross-border payments, and does not support any other transaction currencies only US dollar.  
U.6 Applicability to Multiple Use Cases – Somewhat Effective, Challenges with cross-border use case |
|-------------------|----------|--------------------------------------------------------------------------------|
| Other Stakeholders | Efficiency | EFFICIENCY  
E.1 Enables competition – Somewhat Effective, challenges as integration process is not described.  
E.3 Implementation timeline – Not Effective, project timeline success is dependent on the substantial participation of a network of FIs, without a projected cost impact for an FI to participate.  
E.7 Exceptions and investigations process – Not effective, a formal resolution or dispute process is not available, and there is no intention to develop a process unless is absolutely require by banks.  
The customer enrollment process is sufficiently involved to enable the benefits of insured security. Identifying oneself to one’s bank and installing an app on a smartphone or PC are no more “burdensome” than opening a new bank account, and probably less so. Usage of the system involves each user having two certificates: one establishing identity, the other establishing authority limits. The identity certificate is theoretically mobile, the authority certificate is not because each bank has its own policies to enforce. A consumer must visit a bank branch to establish a new account at that bank, and there is no reason new certificates cannot be issued at that time. Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA. 
The SDK/API will be available to legal licensees of our solution. Its usage will be governed by the license terms. Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. Some explanations involve intellectual property that we are willing to disclose only under NDA. |
<table>
<thead>
<tr>
<th>Other Stakeholders</th>
<th>Safety &amp; Security</th>
<th>SAFETY AND SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S.1 Risk Management – Not Effective, proposer states that risk can be mitigated through insurance coverage (protection), which would be difficult to entice participants to be part of this solution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.2 Payer Authorization &amp; S.3 Payment finality – Somewhat Effective, payments are irrevocable and disputes can be addressed in a “court” system, this will be difficult for any participant to adopt.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.4 Settlement Approach – Somewhat Effective, a trusted settlement account is required for by FI's with transaction settling in 15 seconds, and can be map to the central bank settlement, adding 5 more second the transaction and configuring messaging.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.5 Handling Disputes – Not Effective, no formal process is in place, their approach is to let the FI's dispute among themselves, and if needed form a committee to address these issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.6 Fraud Information Sharing – Not Effective, no information is provided and no plan in place.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.8 Resiliency – Not Effective, key critical items (e.g., required to have their own BCP and DRP for their nodes) are left to the participating FIs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Stakeholders</th>
<th>Speed</th>
<th>SPEED (FAST)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F.1 Fast approval &amp; F.2 Fast clearing – Somewhat Effective approval time is longer than the require 2 seconds, is 10-15 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>F.4 Fast settlement among depository institutions &amp; regulated non-bank account providers – Somewhat Effective, mapping the TSS system to the FI's Federal Reserve bank accounts &quot;may have negative impact&quot; on settlement due to operating hours.</td>
<td></td>
</tr>
</tbody>
</table>

|                  | Our unique transaction insurance does not merely mitigate risk: it eliminates it. Lloyds would never have underwritten our solution unless all but a tiny, residual risk were eliminated by the solution itself. After more than a year of rigorous evaluation and scrutiny, Lloyds knew that was the case and made their underwriting decision. This insurance is now also available from U.S. underwriters for sufficiently secure systems. Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. The legal framework underpinning the solution guarantees legal finality for transactions. A transactor must confirm the transaction at least twice before it is executed. |

|                  | The 15-second average INCLUDES clearing and settlement with legal finality, not just “approval”. The payment feasibility request and corresponding acknowledgement to the payer system takes 2 seconds to complete. This step constitutes approval. On average, it takes an additional 13 seconds to complete the full end-to-end payment process. |

22
| Other Stakeholders | Legal | LEGAL  
L.1 Legal framework – Somewhat Effective, the proposers’ addendum contradicts the “FPTF framework” and they stated they will provide details on a NDA. | Full legal explanations involve intellectual property that we are willing to disclose only under NDA. |
| Other Stakeholders | Governance | GOVERNANCE  
G.1 Effective governance & G.2 — Inclusive governance - Somewhat Effective, if governance is required, it should be provided by government regulators such as the Federal Reserve, FDIC, and OCC. | Governance should include a formal mechanism for the input of the governed to the process of answering questions and deciding issues. |
| Small Financial Institutions | Safety & Security | need to strengthen dispute resolution capabilities/rules | Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. |
| Governance | Details need to be provided. Some statements seemed to be contradictory | We view governance as the role of the regulators. Our intent is to show maximum ability to conform to the eventual governing body’s requirements while offering innovative governance technologies. |
| Medium Financial Institutions | Ubiquity | I think ubiquity is the Achilles heel of this proposal. From a security aspect, sending software by mail or allowing download over a bank's network really enhance security, but if you have a widely disbursed customer based, especially if it is global, the expense and logistics of trying to manage sending items might be hard to make. If there’s a way to make accessing the necessary software easier (you don’t have to mail anything or force someone to come into a specific location), I think then it would have much better appear. | The point is well taken. There may be instances which require special handling. Such problems and solutions will be addressed as they may arise. But for banking in the U.S., it is a one-time effort and not as difficult as it may appear. How many replacement debit/credit cards to banks issue when there is a large breach or smaller fraud? This procedure is not that unusual for a cybercrime-free online banking experience, or for sending and receiving payments in real-time.  

Our proposal does not require a user to go to a bank branch to register unless they want to download the client app over the branch’s dedicated Wi-Fi. Users may load the app from a CD or USB key supplied either by the bank or by InterComputer. In our case, CDs or “jump drives” contain NO SECRETS OR CERTIFICATES, merely client app code. The client app will only function over an ICN connection, insuring security for any secrets or certificates. |
| Medium Financial Institutions | Ubiquity | Limiting participants to requiring them to have a bank or credit union account restricts access to the system. Having a solution to address that would be beneficial. Entrance to the system seems very cumbersome, especially for special needs end users. The more complicated the user experience, the less adoption success. |
| Collected from | 24 |
| Page 47 of our proposal discusses the unbanked in connection with smartphones. Even today, most low-price or free-phones for the low-income are smartphones. InterComputer has patented, proprietary technology that fully delivers all of our solution benefits to the unbanked, but we think it best that this discussion occur after certain fundamental policies that are out of our control have been set. The customer enrollment process is sufficiently involved to enable the benefits of insured security. Identifying oneself to one’s bank and installing an app on a smartphone are no more “burdensome” than opening a new account, and probably less so. |
| Medium Financial Institutions | Safety & Security | Handling disputed payments is a major concern, especially among FIs. Addressing this in the solution would be critical. |
| Collected from | 24 |
| Dispute handling viewed in the traditional sense is obviated by our solution. Nevertheless, we have explained our flexibility in providing mechanisms that deliver the same function. |
| Medium Financial Institutions | Speed | Concerned about settlement speed and the perceived need to be part of the ICN to receive faster settlement. |
| Collected from | 24 |
| The 15-second average INCLUDES clearing and settlement with legal finality, not just “approval”. The proposal did not break down the feasibility request/approval into the two second average for the step. |
| Medium Financial Institutions | Governance | Would have appreciated more concrete ideas on the governance that would make this solution a great approach. |
| Collected from | 24 |
| We view governance as the role of the regulators. Our intent is to show maximum ability to conform to the eventual governing body’s requirements while offering innovative governance technologies. Details will emerge. |
**Faster Payments QIAT**

**FINAL ASSESSMENT**

**Proposer:** InterComputer Corporation

**Summary Description of Solution:**

The InterComputer Network (ICN) is an Internet protocol-based, end-to-end payments solution that supports real-time payments. By relying on its own operating system in a closed network and layering this with additional security, it provides a secure environment for payment delivery. While it is IP-based, the solution is not accessible via the World Wide Web and therefore is protected from the risks that this accessibility would present. ICN manages user identities and authority with proprietary digital certificates. It enforces these with three-factor end-user authentication that includes user name and password, digital certificate, and biometric validation (which not only boosts the solution’s security, but also increases the number of end-user actions needed to authenticate each and every payment).

The solution requires two contracts to be in place to support enrollment: one between the bank and ICN, and one between the bank and its customers/end-users. Banks that wish to participate in the solution must install the ICN’s operating system and its Trusted Settlement System (TSS) application. The solution relies on the relationships among all participating banks to support real-time settlement through the establishment of a new “correspondent bilateral system” among all banks that wish to be in the system. End-users can access the solution through an application called Private Line that enables interaction with the ICN through a smartphone, tablet, or PC. Private Line includes PL Pay (which supports all transaction types) and eCash (which links FIs and their customers). End-users’ payments within ICN are validated, cleared, and settled within 15 seconds. These payments are all irrevocable credit-push payments.

**EXECUTIVE SUMMARY OF THE PROPOSAL**

- **Major strengths**
  - The ICN is a highly secure solution that operates as a closed-loop system on a private network. Payment transactions require three-factor authentication to support initiation (i.e., user name and password, biometric confirmation, and a digital certificate unique to the end-user). Payers must also confirm a payment prior to sending and review terms and conditions for every transaction. All payments are push payments and irrevocable. The solution is insured by Lloyds of London.
  - The solution’s flexibility also supports many useful features. It allows end-users to make exchanges across several interfaces and to set up a hierarchy of accounts for making payments. If the preferred account is short of funds, ICN moves to the next account to complete the transaction, although it does not address the authorizations that would need to be obtained for this. As a closed network, it can monitor the status of payments very efficiently. By relying on the Application Program Interface (API) for integration, the solution can work with treasury management systems, accounting systems, ERP systems, and small business systems (e.g., QuickBooks). Its messaging format leverages ISO 20022. This flexibility – as well as ICN’s scalability – offers significant potential for customization.

- **Areas for improvement and enhancement**
  - Broad deployment in a reasonable time frame (18-30 months) will require strong regulatory impetus from the Federal Reserve and other banking regulators (p. 41) and thus seems unlikely.
– The solution bases itself on completely new, patent-protected technical and business models that are not thoroughly discussed in the proposal, which makes assessment difficult.

– The solution does not offer a governance framework and proposes that if governance is required, it could be provided by government regulators such as the Federal Reserve, FDIC, and OCC (p. 57).

– The solution does not outline how the deployment and operation of this new payment system will be funded. Further clarification of the costs to be incurred by participating FIs and end-users is needed.

– The customer experience in the ICN seems quite burdensome. To enroll in the solution, consumers have to receive a CD or USB stick with the Private Line application in the mail. They must authenticate themselves for every transaction with a biometric identifier and a password. Transactions must be confirmed two times before sending, regardless of the transaction type or value. Unbanked end-users or end-users who are customers of banks that are not participating can register with ICN directly, but sending and receiving of payments will rely on ACH and will not be real time.

– The solution does not settle in central bank funds but rather re-uses commercial bank funds exchanged between participating FIs.

– ICN does not seem to adequately address risk management, and gaps exist in the proposed legal framework. The solution does not consider exceptions and dispute handling. The proposal does not sufficiently explain how the solution would store and share fraud information, or how it would deal with a security breach. The proposal states that presenting the terms and conditions twice during every payment process will eliminate any transaction risk related to errors. Any disagreements that cannot be settled amicably are to be addressed through the court system. The evaluation criteria suggest that a more formal dispute process is preferred.

Use cases addressed


Proposer’s overall ability to deliver proposed solution

– It is not clear that the value proposition for FIs is compelling enough to support the target market share described in the proposal. It is likely that, as the proposal acknowledges, a strong regulatory impetus will be required to support adoption. The implementation timeline is extremely aggressive and does not seem to consider the complexities of designing and implementing the solution at the numerous banks that would be required for ubiquity.
**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 ICN is accessible to customers of any enrolled bank or credit union. It uses an Application Program Interface (API) to support the enrollment of FIs and their customers. The solution can also initiate payment instructions with ACH and Fedwire, ICN Private Line Payments can be accessed from any device.

End-users whose banks do not participate in ICN cannot register. They must move their account or open an account at a bank that participates in the system. End-users can register with ICN directly but can only transact with other, directly-registered users. For these users, the available transaction set is limited, and payment instructions related to sending and receiving payments are processed using an ACH network (U.1.2, U.1.4).

The desire to avoid the risks and cybercrime associated with web-based online banking will help drive adoption, the proposer believes. One of the motivating factors for FIs to participate will be a reduction in the high costs associated with securing web-banking solutions, as well as the ability to offer customers “the ultimate” in digital security. The proposal maintains that FIs are spending “vast sums of money attempting to secure completely unsecurable, web-based online banking (Proposal Q&A p. 5)” and maintains that the installation of ICN’s PrivateLine software will virtually eliminate these costs. Any additional drivers of FI adoption should be clearly described.

The implementation timeline described in the proposal is aggressive at 18 to 30 months. The proposal acknowledges that the proposed timeline is only achievable if the Federal Reserve and other regulators provide a strong regulatory impetus (p.40) (U.1.5).

**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 effort required for banks to set up the solution is not insubstantial. Banks must implement the “PrivateLine Control Bridge” to provision employees with digital identity certificates and authority within the solution, provision customers and determine authorities, and provision applications that will be used as part of the solution. Setting up the existing user base for the first time to generate digital authority certificates is challenging. An existing customer base can be converted to PrivateLine branch by branch. Once created, certificates are easily modified to reflect any changes in information, accounts, and authorizations.

For end-user registration, the bank sends the user the client side of PrivateLine (PL) in physical media format (CD, USB key or Micro SD card) via postal mail. Web-based download is not permitted. Physical media is only needed to support registration and is no longer required once provisioning is complete. The ICN is accessible via multiple devices (computer, tablet, and smartphones) through the PL application. The solution is available 24x7x365. All transactions are push transactions; end-users must actively accept the terms and conditions associated with every transaction. Connections between end-users are established through a connection request sent to another individual or an entity. Entities can determine how they can be searched on the
system. Receivers must accept connection requests before payments can be exchanged. An entity’s “real name” is the primary attribute for searching, connecting, and paying, but email addresses or telephone numbers can be added to the profile if desired.

The end-user authentication and transaction approval requirements result in a lengthy payment experience, and while proposers see this as the necessary balance between security and convenience, this may inhibit some end-users from using the ICN.

The system also provides notifications.

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 ICN is a fully detailed, secure, and controlled payment process with disclosure. It also supports a consistent end-user experience across channels. The same user interface and the same payment processes (from initiation to settlement) occur for every transaction. The end-user application is “Private Line,” and “PL Pay/payment” is the branded solution.

The proposal supports the sharing of fees associated with a transaction through the use of a configurable field, or by adding language to the acceptance screen, but there is not a requirement to inform end-users about fees before the payment occurs (U.3.2).

The proposal does not describe error protection rights. Disputes that cannot be amicably resolved between the payer and the payee must be settled outside the payments system in the courts. The ICN does not allow for payment repudiation either (p. 27) (U.3.5). The proposer states that ICN can offer a “dispute resolution” process if banks require it.

The solution’s name is “PrivateLine Payments.” A Private Line label or icon will be available for merchant locations to inform end-users that they can make real-time payments at that location.

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
Contextual data may be exchanged in all ICN transactions. Associated messages, regardless of format type, arrive in real time with the payment message. Enrolled business users, for instance, can connect their accounting/purchasing systems to ICN and initiate PL Payments directly from their business application. Business partners can leverage an InterComputer solution called PrivateBusinessDrive to exchange large contextual data files independently of the payment. The proposal states that all messages within the ICN use ISO 20022 XML syntax. It further states that mapping to non-standard applications can be developed in weeks if this capability is required to facilitate contextual data for payments.

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 ICN currently views cross-border functionality as both a mid- and a long-term priority. In the mid-term, it can extend the TSS to international banks and leverage the same legal agreement to do so. The solution does support payments made in currencies other than the U.S. dollar. Large banks dealing in multiple currencies can directly send or receive payments to and from international banks that also use PrivateLine. The ICN will need to offer more transparent pricing and conversion details for its international end-users (U.5.3). Over the longer term, the solution proposes to build direct TSS and banking relationships with global banks and will share fees with them.

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

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

**Rationale:**
The ICN supports all use cases, including B2B, B2P, P2B (including POS), and P2P.

**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:**
Any bank or credit union can participate in the solution as long as they sign the required agreements, implement the TSS capability, and join the Payment Legal Network. If the FI does not want to implement the TSS, ICN can host it for them. ICN will make its API available to FIs, corporate entities, and developers to allow them to develop new solutions.

The proposal states that FIs can brand and price PL Payments without any constraints defined by InterComputer. There are a number of parameters that are defined by the individual FIs in their implementations of Control Bridge and deployment of the solution (account types, transaction amounts etc.), but the end-user experience and access to the system seems to be very tightly controlled by ICN and supported by standard agreements to be signed by all participants. If end-users wish to change banks, their original bank revokes their digital identity, and they must register with the new bank to obtain a new digital certificate.

The proposal indicates that an InterComputer SDK is available to adapt existing solutions to the ICN, or to create new solutions that can be integrated with the ICN. The process for the integration of new services is not described.

The solution can support the disclosure of fees in advance of a transaction but does not require this disclosure. A configurable field can be used to display fees in advance. Alternatively, fee information can be added to the legal language that is presented on the transaction acceptance screen.

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

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:
The ICN allows enrolled FIs to develop and offer additional value-added services to their customers. The ICN Software Developer Kit provides gateways for providers and other software developers to create applications that run on the ICN IOS. In the proposal as written, it does not appear that non-banks are able to develop value-added services. The proposal states that making value-added services optional, as well as the disclosure of any fees, is the responsibility of the service provider (E.2.3).

E.3 Implementation timeline

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

Rationale:
The solution outlines a very aggressive implementation plan. The 18-month timeline allotted for key implementation activities at each FI may not be sufficient. Details are not provided for each major activity. It is not clear how many FI participants are needed to deliver scale. Success will require a substantial network of participating FIs. The implementation plan states that FIs should absorb the implementation costs but does not quantify the investment required for an FI to participate.

The 18-month estimated for implementation at an individual bank includes testing. The proposal claims that 90% of ICN technology is common to all implementations, and only 10% is custom technology.

The proposal suggests that within two years, the solution could have 25% market share, and within three years, 50% market share. This timeline does not consider any regulatory approvals that may be required. The proposal states that the implementation timeline can be more effectively estimated following adoption at a major bank and suggests that “market share” refers to the number of banks participating in the system.

Participating FIs will be supported by ICN integration teams that work with banks’ IT staff to define requirements and determine schedules. The proposal states that banks’ IT staff can train and provision branch employees without InterComputer assistance. The role(s) of business and operation staff in the deployment process should be described. To support community banks and credit unions, the proposal suggests that third-party providers could act as integration partners. The implementation plan does not describe the development and implementation effort required to support settlement in this system. The creation of a new correspondent banking network will almost certainly be time-intensive and will require investment and support from FIs.

The proposal acknowledges that this aggressive timeline is only achievable if the Federal Reserve and other regulators provide a “strong regulatory impetus.” Experience has shown that similar transformations – those that hinge on regulatory actions not currently under consideration – have required a much longer timeframe.

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 ICN leverages the ISO 20022 standard for its transactions and applicable contextual data. ISO 20022 is widely interoperable, can accept free form text contextual data, is cost-effective, and is quite flexible. The solution will have the flexibility to support multiple payment standards and can develop new communication formats as needed to support contextual data requirements.

E.5 Comprehensive

**Very Effective**  Effective  Somewhat Effective  Not Effective

Rationale:
The solution addresses and handles all aspects of the end-to-end payment process from initiation to reconciliation. The ICN’s technical design supports all of its features, including its information security protocols, compliance and risk controls, and reliability (among others).

E.6 Scalability and adaptability

**Effective**  Somewhat Effective  Not Effective

Rationale:
Thanks to ICN’s distributed technology architecture, the solution’s hardware and software can scale globally as system volumes grow. Only ICN’s hardware and bandwidth limit its speed and usability. The proposal does not describe the solution’s capacity to handle projected volumes and values, projected throughput (TPS), or the impact of provider growth and transaction volume growth on transaction speed (E.6.2). The provider is committed to 99.9% availability, which is supported by off-site hot site mirrored server capability. Any bank that participates in the solution is required to meet the same availability target. InterComputer can provide off-site hot site mirrored services for banks that prefer it.

E.7 Exceptions and investigations process

**Effective**  Somewhat Effective  Not Effective

Rationale:
The solution has thorough security and fraud prevention measures. By requiring payers to confirm payment details twice before executing a payment, the solution aims to minimize transaction detail errors. While there are clear provisions for system audit, forensic audit, and the ability to examine any one transaction or multiple transactions from the Control Bridge, there is no formal error resolution or dispute process to address errors that do occur and no tools or mechanisms are described that will assist in the resolution of errors or disputes. Lack of a formal dispute process may hinder adoption (E.7.1). The proposal does indicate that a dispute resolution process can be developed if participating banks require it.

Authorized personnel and their specific roles will be defined with FIs as part of the installation and requirements-mapping process.
The ICN stores all transaction information in the TSS Ledger and will retain information as mandated by the applicable financial regulatory agencies. The ICN does not aggregate information across providers in order to detect patterns (E.7.3). Reporting requirements will be specified in non-disclosed SLA conditions.

**Safety and Security**

**S.1 Risk management**

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

**Rationale:**

The proposal states that the solution’s reliance on push payments, technology, and authentication mechanisms will prevent all or most systemic risk. The solution is flexible and can accommodate changes in law or legislation that may have an impact.

The solution has no processes to handle exceptions or resolve disputes (S.1.4). Although the ICN plans to reduce operational risks through its distribution and technological set-up, these measures do not credibly deal with all potential risks (S.1.3). The solution should include features to address payment-related risks, including risks related to account set-up; bilateral, non-collateralized settlement; and denial of payments (S1.1-S.1.4). The proposal does not describe incentives for operators and providers to address and contain the risks they pose to other participants (S.1.5).

The proposal states that residual risks have been addressed through insurance coverage. A Transaction Insurance product was created for InterComputer and its customers in ~2005. This insurance protects “all organizations, employees, and customers of organizations which have been provisioned or registered to ICN according to established procedures and operation of the PrivateLine Control Bridge and ICN requirements (Proposal Q&A p. 13).” Details of the insurance policy are provided in the proposal. The proposers maintain that this comprehensive Transaction Insurance is only possible because the residual risk in the system is so low. The proposal does not explain in sufficient detail why systemic risk is so low, nor does it describe how these low risk levels can be maintained.

**S.2 Payer authorization**

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

**Rationale:**

The solution requires the payer to undergo three-factor authentication prior to initiating a payment, and then the payer must review each transaction (with its terms and conditions) twice before sending the payment. The solution supports pre-authorized push payments and does not support pull payments of any kind. Once a payment is executed, it is irrevocable.

**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:

Each bank enrolled in the ICN signs the same enrollment agreement, which establishes three foundational obligations: participating banks must agree that every completed PL Payment is legally final, binding, and non-rescindable; the bank’s customers must be bound to the same terms and conditions; and the payment becomes irrevocable 10 to 15 seconds after the payer confirms the payment for the second time.

The solution does not currently include any defined mechanisms to support a disputed payment (even one made in error). Parties to a dispute are required to settle their differences amicably; if they cannot, their only recourse is to take their claim to the court system (S.3.3). The proposer has indicated that the technical details supporting the absolute legal finality of transactions, as well as the immediate availability of funds, are covered in detail in their patent.

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:

Every participating FI has a Trusted Settlement System (TSS) account. The FI can hold this account on a TSS server, or a third party may manage the account on the bank’s behalf. All payments in the system are push payments. The payments process involves confirming that good funds are available in the payer’s DDA account, transferring the funds from the payer’s DDA to the payer bank’s TSS account, transferring the funds from the payer bank’s TSS account to the payee bank’s TSS account, and transferring the funds from the payee bank’s TSS account to the payee’s DDA account. All of these transfers occur in less than 15 seconds.

While settlement occurs in commercial bank money, the solution manages the risk through irrevocable push payments and legal agreements between the participants and end-users. The establishment of official commercial funds is contained in a non-disclosed SLA, which every bank on the system must agree to meet. The solution can also support settlement in central bank money by mapping the TSS system to the bank’s Federal Reserve account. This implementation would require additional messaging and would add a few seconds (5) to the transaction time.

If an FI in the system should fail, the InterComputer Network would immediately revoke the bank’s certificates to cease their operations on the system.

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 ICN is designed to limit the occurrence of disputed payments, and the proposal as written does not define any role for the solution in handling disputed payments. It denies any liabilities in this area because the solution trusts that its technology will avoid any such incidents. As a result, the proposal does not contain any procedures, mechanisms, or considerations for handling disputes or protecting business, government, or consumer payers. Instead, the payer or the enrolled FI is responsible. The payer can request a voluntary return by phone, email, or a chat platform but has little recourse beyond regulatory compliance. The proposal does state that a dispute mechanism can be developed if required by participating banks (for “payments made
in error,” for example). In this case, the SLA would be updated, distributed electronically, and digitally signed by all participants. It is suggested that a committee be created to develop any dispute rules.

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 ICN believes that collecting fraud data in real-time systems is ineffective (page 29). Instead, if the ICN system detects suspected fraud, it immediately suspends the digital credentials of the user in question. The ICN, the owner of the TSS, is currently the only entity able to monitor all transactions in the system. The proposal states that the system already contains a centralized fraud monitoring capability and in effect provides fraud information-sharing in real time. This information is available offline to participants for fraud management purposes. Rules can be added to the system as required and defined. The system does not require participating FIs to monitor their transactions for potentially fraudulent activity, but since all participants can allow others to see their data, broader systems can be developed.

As the effectiveness criteria suggest, a fraud monitoring capability is beneficial. InterComputer might consider revisiting its stance and developing or providing a monitoring capability to ensure that all end-users and transactions in the solution are legitimate.

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 ICN solution provides a secure environment with multiple levels of security and encryption. The network has protected links and equally strong nodes. The secure message transfer system validates and exchanges secure messages in real time. It also ensures an audit trail of all transactions. It would be beneficial to providers if the solution defined minimum requirements for user enrollment. The technical security to support enrollment is unclear.

The proposal as provided does not define any requirements regarding server hardware. The core messaging software (i.e., IC iOS) will only run as fast as the available CPU power, memory, and storage space allow. It would be helpful for the proposal to describe how participating FIs will manage and oversee the interface between the ICN and their risk management processes, legacy payment infrastructures, and end-user interfaces.

S.8 Resiliency

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

**Rationale:**
The proposal indicates that the solution’s target availability is 99.9%, which is supported by off-site/hot-site mirrored capability. All participating banks in the system will have the same availability requirement. With regards to DRP (disaster recovery planning) and BCP (business continuity planning), the solution states that InterComputer has BCP and DRP in place, along
with a system testing schedule, as required by their underwriter. Participating FIs are required to have their own BCP and DRP for their nodes and to comply with any SLA security practices. More detailed information describing the underwriters’ requirements and how these are satisfied would be helpful. ICN commits to build capacity 25% ahead of demand, but does not clarify how this demand would be forecasted.

S.9 End-user data protection

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The ICN requires operators and providers to use robust mechanisms (e.g., high-level encryption) to protect information (both end-user and employee) in the end-to-end payment process, including the protection of shared data (e.g., the ICN digital certificate). The proposal states that ICN requires operators to comply with data protection requirements as defined in the Service Level Agreement, but does not articulate what these requirements are.

S.10 End-user/provider authentication

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution leverages ID verification (ID+V) and Know Your Customer (KYC) requirements for opening an account at a participating FI. End-users initiate all payments with three-factor authentication, which requires their user name and password, biometric identification, and their digital certificate. The solution automates full compliance with relevant regulatory guidelines.

S.11 Participation requirements

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The proposal indicates that any FI or credit union can participate in the ICN. The legal framework is set up through a law firm, and participating requirements are managed through a contract signed by every participating FI. Details are only available under NDA (non-disclosure agreement). When an FI becomes a participant, it must undergo a security review. Annual security audits are also required. InterComputer monitors the TSS system constantly for overall system compliance. Additional participation requirements are defined in the SLA, which is available upon signing an NDA.

Speed (Fast)

F.1 Fast approval

Very Effective  Effective  Somewhat Effective  Not Effective
Rationale:
The solution takes 10 to 15 seconds to execute, clear and settle – the feasibility request and acknowledgment (approval) takes two seconds. According to the Task Force’s Effectiveness Criteria for fast approval, a process that takes within two seconds earns a “Very Effective” rating requires approval within two seconds.

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 clearing of debits and credits is almost instantaneous, earning the solution a “Very Effective” rating for Fast Clearing.

F.3 Fast availability of good funds to payee

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

Rationale:
The solution takes somewhere between 10 and 15 seconds to make Good Funds available to the payee. According to the Task Force’s Effectiveness Criteria for fast availability, a solution is rated “Very Effective” if it provides good funds availability within one minute.

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

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

Rationale
Real-time settlement within the ICN, where the TSS exchanges commercial bank funds, would occur within 10 to 15 seconds. Transactions are settled as each entry is cleared—which happens almost instantaneously—but only after all acknowledgement messages have been received end-to-end does settlement become official. This process takes about 10 seconds. The real-time settlement option is fully insured and must be available 24x7x365, which prevents lag.

The solution suggests an implementation option that would map the TSS system to participating banks’ Federal Reserve accounts. This implementation could negatively affect the speed of settlement, as the Federal Reserve does not operate 24x7x365. The solution does not describe how settlement lag will be managed, including management of settlement needs of banks in various time zones.

F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:
The TSS notifies the payer’s and payee’s FIs as soon as a payment has been initiated and received. The FIs can then notify the payer and the payee. The ICN has not set requirements for the timing of these notifications.

Legal
L.1 Legal framework

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

Rationale:
The Legal Framework in Addendum C of the proposal describes how participants are legally bound to the ICN but does not cover some of the important areas in the FPTF framework. The Addendum does not describe how entities in the system will be legally bound. The proposal describes the legal and regulatory obligations that will govern the operation of the ICN; compliance with many of these obligations is automated and automatically enforced by the solution. The solution’s SLA contains “terms and conditions of use, requirements for use, and the legal language to create absolute, legally binding finality between banks and their customers that register for the solution (Proposal Q&A p. 23).” The proposal states that additional details regarding the solution’s legal framework are available under NDA.

L.2 Payment system rules

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

Rationale:
The proposal addresses key features of the solution and describes obligations set forth by the legal framework. Addendum C summarizes the rights and obligations of the participating banks and end-users, while the legal framework concentrates on payment irrevocability. No processes for error resolution are provided. The proposal states that a committee can be established to address ongoing issues related to payment system rules (governance, abuse, regulatory concerns, etc.). This committee would approve all changes, which would result in the updating of software and SLAs as required and the subsequent roll-out to all participating FIs.

L.3 Consumer protections

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

Rationale:
Addendum C, which the ICN cites as its source for consumer protection, summarizes the rights and obligations of the participating banks and end-users, while the solution’s legal framework concentrates on payment irrevocability.

It is suggested that the proposal allocate legal responsibilities for payer and payee losses in the case of disputed payments (L.3.1) and establish payment system rules and procedures for error
resolution (L.3.2). It should also consider setting up additional consumer protections and/or supporting payee and payer claims due to fraudulent activities or end-user errors (L.3.3). In the event that consumer protection is required, the Bank TSS Committee will provide input and feedback. The TSS will be modified if required to deliver the additional customer protection requirements. Bank SLAs will also be modified.

L.4 Data privacy

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

**Rationale:**
The proposal states that PrivateLine and the TSS do not permit data collection on either personal or organizational transactions. Payer or payee payment data is accessible only to the payer, the payee, and their respective banks. Contextual data is only accessible to the payer and payee. If a government agency requires contextual or payment data, the request must be made using the required authorized legal documents. The proposal does not mention any policies on end-users’ access to their own data, nor does it describe ways in which end-users can limit the data/information collected on themselves or manage their own data privacy preferences. If a data breach is attempted, alerts are sent to all parties, and continuous system audit capabilities are engaged. The solution also seems to lack processes for surfacing, escalating, and dealing with a data breach (L.4.4).

L.5 Intellectual property

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

**Rationale:**
The solution has a clear proposed approach to resolve and manage any risks arising from third-party intellectual property rights (prior to implementation). The proposal mentions several patents and patents pending, but a legal assessment of ICN’s IP has not been conducted.

Governance

G.1 Effective governance

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

**Rationale:**
The ICN operates under a distinctive premise with regard to effective governance. The proposal states, “The nature of the PL Payments solutions obviates the need for participatory rule-making by providers and/or users. Allowing such activity could destroy the inherent security of the system and nullify transaction insurance coverage” (p. 57). If governance is deemed necessary, the proposal suggests that the Federal Reserve, the FDIC, and the OCC could provide governance. These three bodies could listen to suggestions or recommendations from providers and users for system enhancements, the proposal says. This level of governance is not currently applied to low-value payments.
The proposal does not describe any governance disclosures or appeals process. The proposer does, however, recognize the need to establish a committee or group containing representatives of all stakeholders to ensure that customers have an opportunity for input. This body’s formal role is not articulated in the proposal.

The Effectiveness Criteria call for effective participatory governance over the processes listed in previous sections of this assessment and in G.1.

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:**

Regulators and rule-making bodies typically establish rules and/or standards to minimize risk, determine the liability of participants, and provide end-users with recourse and/or reimbursement. The proposal indicates that, regardless of potential regulator involvement in solution governance, an independent governance group consisting of FIs and industry participants will be created. The group—envisioned as a diverse collection of bank representatives from large, regional, and community banks as well as credit unions—would meet to discuss issues that pertain to rules or functionality required at the bank level and/or the end-user level.

If such a group were created, the ICN might consider re-evaluating its stated stance and adopting an approach to both effective and inclusive governance. This approach need not compromise the ICN’s system and insurance to meet the criteria for effective governance.