November 7, 2019

Ms. Ann Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington DC, 20551

<<<Submitted via email to: regs.comments@federalreserve.gov >>>

Subject: Comments on Potential Federal Reserve Actions on proposed RTGS Payments,
Docket No. OP – 1670

Dear Ms. Misback:

The U.S. is challenged by fast, cheap internet connectivity and the pervasive use of the World Wide Web for mission critical purposes. Connectivity and 'the Web' are not inextricable. The original developers of internet TCP/IP and Web protocols did not consider security and privacy in their designs. As a result, identities and data are at constant risk of exploits and represent the current environment and a growing problem.

At this point in time, critical digital interoperability is required throughout the United States – not only for real-time payments – but every other interoperable process – all activities that lead up to a payment.

To achieve this goal, superior safety and trust must be utilized with a secure messaging system which is internet based for ***accessibility***, and can be separated from the risk-prone web with its unnecessary attack surfaces. Purpose-built digital messaging software designed and built from the ground up with security in mind for the internet is required to provide unpolluted, exact security and privacy, with ***continuous*** digital trust within and between organizations and consumers.

At the same time, there is a strong need of lower IT security costs and dramatically increased productivity across all economic sectors which is yet to be realized. This increase in productivity cannot be achieved with the web. The web was designed and built to share information, not secure it or keep it private. Trying to secure it "after the fact" is contrary to correct technological principles in the software design and development process.

During the FPTF period, Governor Powell and Governor George on several occasions emphasized that "safety and soundness" is the primary concern of an RTGS system to achieve the Fed's goal of "ubiquitous real-time payments." As a first priority the logic is solid.

INTERCOMPUTER CORPORATION

2989 W. Maple Loop Dr.
Third Floor
Lehi, UT 84043

Phone 801-849-1440
www.InterComputer.com

Functionality must be preceded by safety considerations in internet software, and cannot follow it, or the lack of digital security required to achieve and maintain it will prevent banks and their customers from using it. There are sizable productivity gains in velocity of funds to be realized by doing it right.

Economically, the U.S. must become far more productive for the economy to grow and the nation to prosper. Digital superiority is required. Data security and privacy cannot be legislated. Cyberthieves do not honor law.

The current digital dilemma of using the World Wide Web for purposes it was not designed to achieve, can be summed up from these words from the film *WarGames*:

*"**Greetings Professor Falken. . . A strange game. The only way to win is not to play**." (Joshua-WOPR or the computer's conclusion of simulated global thermonuclear war.)* Eyre R. (Producer), Craig G. (Producer), & Badham J., (Director). (1983). War Games [Motion Picture] United States: MGM.

The Fallacy of Encryption Working Alone

Encryption working alone without separate software layers of protection is only hiding data, which is an essential technology principle to understand. To quote an expert, ***Encryption is obscurity and obscurity is not security***. Solutions relying on encryption alone cannot be relied upon for unpolluted, exact security and should be not be so used. There is always someone or entity that can break it or find other ways around it.

Oddly, most security components in computer science during the past three decades have focused heavily on encryption methods and techniques for computer security. Pseudo-terms like "quantum-safe" are being applied to encryption methods to try to associate it with the still impractical use of quantum encryption, which is separate from quantum computing.

Encryption must be used in protecting data, but not relied upon. Other software layers of protection must be used in conjunction with cryptography to provide an internet messaging system which can be relied upon and result in unpolluted, exact security and privacy. Certainty, from end-to-end must be present.

The FPTF Sub Work Group – Interoperability comprised of payments industry luminaries having the common concern about "open web based" API's being utilized for interoperability between multiple RTGS operators and transactional activity on multiple systems leading up to the payment.

The concern is valid. Who evaluates the safety of software behind the API? When data is handed off to the next system, how secure is it? Standards defined on paper can be implemented, but vetted by who? Can software code be evaluated and audited regularly? What about maintenance? What about the humans doing work and the potential for human error behind it? Do all humans possess equal capability to deploy software at the highest levels of trust? Are industry best practices on a faulty web adequate to support robust, scalable, safe real-time payments? Do open API's create weak links on a network?

We believe the Fed would do well to re-visit the documents and activities of the Interoperability Sub Work Group in evaluating these questions.

On the subject of interoperability, openness and the web is too loose and closedness is too restrictive. We believe the Fed request for comment document uses the correct term "accessible," which is in the middle of the two extremes. Control over accessibility is key to strike the right balance between open and closed models to make the system usable and reliable with certainty for all.

ICN was built to control and provide accessibility while making it easy to do so, and provide easy accessibility to qualified organizations and consumers to use. ***Certainty*** is the result.

ICN's Model of InterOperability and Accessibility has built-in "completeness" with safety and privacy considered throughout the arc of the design, build and deployment process. Adding safety and privacy functionality after the fact is contrary to security and privacy principles.

The comment document rightly points out that "because of the irrevocable, absolute finality required with real-time payments, the overall safety of faster payments depends in part on how well fraud can be detected and prevented." (Page 52) ICN prevents cybercrime at the outset because the massive attack surface of the web is eliminated. Cybercriminals cannot attack what does not exist. Multiple layers of protection surround the TCP/IP messaging. The ICN model does not rely upon sharing fraud and crime data. Because all nodes on the network are Superior Nodes of Equivalent Strength and must be relied upon for certainty, ICN incorporates standardized software which provides ease of use, combined with low cost and certainty.

What is the Permanent Solution to solve the digital messaging and interoperability problem? The answer is InterComputer Network (ICN). ICN has taken the TCP/IP internet protocol suite, enhanced it, added multiple layers of protection around it, including identity and authority management, all working as a single unit, in "completeness" to protect people, organizations and data.

The permanent solution to the problem of hyper-breach is to re-deploy mission critical applications and processes from the web (and web-cloud) to ICN for business purposes which fundamentally require safety, privacy, exactness and full control by organizations. Going forward, essential applications such as real-time payments should be deployed on ICN. ICN **Business Internet** replaces Web and Email for all mission critical systems which require superior, unpolluted exactness before, during and after information exchange – all the time. ICN gets everyone out of a "losing game."

Real-time, Digital Payments is a Mission Critical Application
The web should be used for what is was built to do when sharing information is desirable. For all other purposes of internet connectivity and interoperability, ICN is the solution. ***Bifurcation of the two is required to achieve all digital goals.***

ICN's architects not only designed for safety and privacy, but for ease of use, low cost and adoption. Multiple adoption methods of ICN enable precise interoperability with exact, verifiable, continuous trust between systems across organizational boundaries.

Among adoption methods, ICN has the capability to import entire websites into the safety of the ICN environment and preserve the http addressing and other website application functionality for any one site or group of sites which may be imported. Browser plug-ins maintain the boundary between ICN and all other internet protocols, such as E-mail, Web, FTP, UDP or others.

Direct mapping between systems whether by coordinating between entities, or connecting to API's are other methods. ICN has a third-party developer program and SDK for qualified organizations. Complete software applications can migrate to interoperate between applications, companies, industries, governments and individuals. Every node on the network becomes a Superior Node of Equivalent Strength and can be relied upon for certainty.

The W3C is an instrument of the major browser manufacturers. The web provides unnecessary attack vectors. Even Sir Tim Berners-Lee recently stated that "the Web is dysfunctional." He cited cybercrime in general, nation-state hacking, perverse data privacy abuse and perverse advertising abuse as the reasons behind this manifest problem.

He and others have been trying to determine methods to protect data, but for an internet software application designed and built to share information universally, considering security after the fact is in opposition to the principle that security and privacy must be designed and built at every juncture of the development process.

ISO 20022 is actually data schema agnostic. There are different schemas that can be used to implement it and the uniform data elements usable in a variety of implementations by different banks and businesses throughout the world (e.g. Tencent's WeChat-Pay). ICN supports using the ISO 20022 data formats. Crucially, ICN is not dependent on using the XML, JSON, etc. web-centric data schema.

An exemplar FedNow Payment Clearing and Settlement Process has member banks adopting the same seven-day accounting regime as the Federal Reserve to maintain symmetry of 24/7/365 and ease of overall operation without evening, weekend and holiday implications. There is time for banks and vendors to make the back-office adjustments as necessary and still experience a relatively quick deployment.

Because bank customers can only initiate push payments when 'good funds' are present in account(s), payments are 'pulled' for 'credit-push' in real-time 24/7/365. If good funds are not in the account(s), even if a "pull" functionality was attempted, the payment cannot be made. Therefore, there cannot be an opportunity to "overdraw" accounts. Similarly, ICN's Trusted Settlement System (TSS) precludes bank customers making payments if there are not any 'good funds' to transfer. TSS supports direct bank-to-bank interbank settlements or via reciprocal ledger entries at a central bank.

Existing bank liquidity mechanisms between the Fed and its member banks can be adapted to the real-time payments service and enable banks to manage it.

Features

There is no reason the Fed cannot begin enabling banks to offer end-to-end purchase to payment features to include remittances either traveling with the payment or at the time of payment over direct connections. ICN is already capable of enabling banks to enable their customers to engage in the digital purchase to payment process on the Business Internet and should be considered. ICN can supply details.

Because ICN can be integrated with **mobile apps**, mobile real-time payments can be completed on the Business Internet with continuous audit capability. There is no point in the payment cycle where completion or non-completion of a payment is ever in doubt. Web or web cloud cannot provide this level of certainty. ICN can supply details as there are considerations unique to ICN to support this claim.

Banks can empower consumer and business customers quickly and easily with protected, insured, mobile capability on ICN, which is exponentially stronger with both connectivity and strong digital identity an authority certificates with many benefits. There are more ancillary and important features the Fed can begin with on ICN and at a much faster timeline than stated in the comment document.

Section V.D. – Implementation Timeline

Three, four or five years is not necessary to make real-time payments available to all banks, credit unions and third-party providers if ICN is tested then adopted. Migrating Fedline to the ICN cloud is easier than trying to deploy in the web cloud with a far stronger result.

1. The software is already built and proven.
2. The software has been vetted by major insurance underwriters and found so effective there is only a residual or miniscule risk that something may go wrong. Nothing on earth is absolute. ICN is the only company to be underwritten for comprehensive cybercrime insurance for customers, even while the data is in transit or at rest anywhere on the internet, so long as it is on ICN. If something should go wrong, there is financial recourse. There is no evaluation or standards body which can meet this high standard. Judgment should not be passed on the volumes of funds transferred in an hour or day on a 20th century mindset. Once understood how it works, there is nothing overwhelming about it. It makes common sense and an important risk mitigation device.
3. The implementation and onboarding hierarchy follows:
    a. The Fed established as host with ICN connected to the FedNow application.
    b. The Fed provisions the twelve district banks. District banks become distributed hosts.
    c. District Reserve Banks provision all FI's in their districts and they become distributed hosts.
    d. Each FI provisions its ops centers supporting multiple branches and business units and they become distributed hosts.
    e. Each branch provisions their customers, both businesses and consumers. (This step is the gate to the last mile.
    f. Once business customers connect either through mapping to custom products or through pre-mapping to major products to serve their needs including PoS, banks will finally be able to enable an RTGS network to serve their customers from end-to-end.
    g. Banks can offer business customers access to B2B, C2B, C2G, B2G,C2G and P2P, whatever the use case.
        i. Included in provisioning are strong digital identities following all KYC rules and backend verification.
        ii. Once provisioning is completed in this hierarchy, directory services can be offered to bank customers who need to look-up then "connect" safely to new business partners automatically and earn a fee. The directory function is inherent in the connectivity made available with controlled authorization and safety.
        iii. This process can be implemented in one-third the time or less than described in the comment document.

ICN has been designed to scale upward limited only by hardware and bandwidth. Because the software is already built and proven, testing and load testing can be done in six months. Provided there is cooperation from the Fed, its member banks and vendors where applicable, the implementation period to the provisioning of all banks and bank customers can occur within the following year after the testing period.

Banks must transform to become digitally sound and modernized. The financial services industry needs a new infrastructure upon which to build for payments, and for every other service to remain healthy and viable in a new world which has become "too brave." The web is 1980's technology, blockchain, tokens and crypto are fallible additions to the web. Banks need a strong, cohesive, reliable digital infrastructure rather than fragmented, weak legacy systems blended with internally developed webware, and the webware fintech's have been selling. This inferior webware is enabling non-bank competitors to act like banks. The Wild West Web is still very rough.

There is a purpose for the World Wide Web to be used for the purpose it was designed, to share information when it is desirable to do so. For all else, ICN should be used for the controlled, precise security and privacy required now and in the future.

FI's also need a lower cost structure to thrive and pass on lower costs to customers. ICN provides the infrastructure to deliver superior connectivity and performance, and to build-on through the 21st century. With strong, continuously audited ICN connections, banks can offer all services digitally, safely, with confidence while bank employees become enabled to service customers in multiple ways. The current fintech environment is built upon 20th century technology and outdated for digital connectivity and secure, private digital messaging functions.

Respectfully,

Scott M. Volmar
CEO