



December 14, 2018

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

Submitted Via: regs.comments@federalreserve.gov

Subject: Comments on Potential Federal Reserve Actions on proposed RTGS Payments
Docket No. OP – 1625

Dear Governors of the Federal Reserve Board:

We agree with the premise that U.S. GDP growth rates can rise by accelerating the velocity of funding and digitalized collateral. Accordingly, we support the notion that the Federal Reserve System operates an interbank real-time payment and settlement system based on the principle of open access which includes being interoperable with other Real-time Gross Settlement systems. We applaud the intent behind the current proposal.

However, before positive outcomes can be harvested by financial account owners and fiduciary institutions, superior and persistent data protection measures must be instrumental in protecting every process, end-to-end. Not doing so will result in rising rather than declining cyber theft rates, resulting in unacceptably high losses in income, wealth, and productivity.

RTGS systems can only be safe, sound and viable if correct technological principles are followed and software is built upon them.

We are concerned that the Federal Reserve System proceed with due and deliberate haste to achieve its objective of open access to the powerful new RTGS capability. We point out that the requisite software framework has been developed to a strict risk-evaluated methodology. We welcome closer inspection. Because a faster, more cost-efficient mechanism already has been underwritten to operate and is proven to answer the challenges of scale with precision and accuracy, it would be unwise to attain this threshold by replication that would incur an unnecessary delay.

ICN is committed to supporting the Federal Reserve System complete its journey to achieve interoperability among RTGS systems. We look forward to serving the Financial Services industry.

Sincerely,

Scott Volmar
President & CEO

Attachment

INTERCOMPUTER CORPORATION

2989 W. Maple Loop Dr.
Suite 300
Lehi, UT 84043

Phone 801-300-3380

www.InterComputer.com



Transaction-centric banking can achieve the fast, convenient, and accessible transaction capabilities necessary to prosper in the digital economy. We discuss how the underlying capabilities for Real-time Gross Settlement (RTGS) can be implemented for wide-spread adoption as early as late Q2, 2019.

Introduction and Rules:

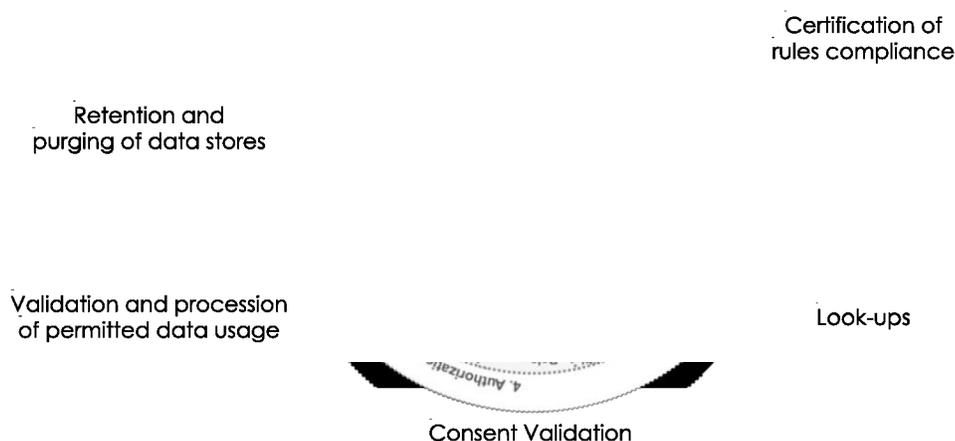
The InterComputer Network (ICN) is extending its proven core InterOperating System (IOS) for tests by pilot banks ranging in asset size from \$50M to \$72B. Each bank will validate new Treasury Management service offerings to institutional Wealth Managers and Family Offices – some compete with larger banks on a peer-basis for transactional revenue drawn from Treasury services.

The ICN Real-time Gross Settlement (RTGS) framework's cryptography empowers the “edge” with client-owned, legally enforceable persistent¹ data protection; comprehensive² privacy protection (data access restrictions); and end-to-end³ confidentiality protection (data usage restriction).

Every event is recorded to a ledger for an end-to-end⁴ Chain of custody. This “business chain” comprises the authoritative record of the atomic settlement process. Each component process must complete before being added to the or (i.e., ledger entry). By rule, superior nodes⁵ can access ledger entries to receive validation messages required by the Gateway Protocol for interoperability.

RTGS event ledger

Fiduciaries validate accuracy of attribute bindings



Originators: a.) attest to the accuracy of Legal Entity Identifiers; and b.) rely upon reliable provenance for the accuracy of receivers' data

¹ Persistent means throughout a digitalized identity's entire life-cycle.

² Comprehensive means every data event and every transfer.

³ End-to-End means the security and accuracy of data's liable provenance is protected in a verifiable manner through every process step

⁴ Insert SWIFT FPS link here

⁵ Superior Nodes means that every node on the network is of superior strength therefore there are no weak links on the network.



2019 pilots:

⇐ 1H 2019 ⇒

- High-Value Real-time Domestic Money Transfers
 - USD-to-USD currency
 - Account-to-Account
- Gateway Protocol – applicable Use Cases
 - Financial management & accounting
 - Treasury and Asset Management
 - User management and administrative tools
 - Financial messaging
 - Asset lifecycles and history
 - Access to liquidity

⇐ 2H 2019 ⇒

- International & interbank payment clearing and settlement
 - Reduction of Fraud
 - Trade finance
 - Regulatory compliance & audit
 - AML/KYC
- Insurance
 - Peer-to-peer transaction risk management

Rationale:

Banks must protect their traditional payments franchise and meet regulatory and treasury managers' demands for speed, safety, and accuracy in payments.

For this reason, ICN's PrivateLine Banking™ RTGS service was created to reduce the chronically vulnerable attack surfaces of web-based online banking. ICN replaces every associated weakness and risk with secure messaging, identity management, authority management, and COMSEC and INFOSEC data protection.

InterOperation challenges between TCH-RTP and FED-RTGS

Meeting regulatory and treasury managers' demands for speed, safety, and accuracy in payments, requires the sender's fiduciary to provide a 'good funds' guarantee that is not impeded by operating rules and can only be enforced within a given jurisdictional boundary. For instance, transfers now can originate within an RTGS system that uses item-by-item rules together with a liquidity management tool instead of pre-funded accounts. It is now practical for a Gateway Protocol to enable the InterOperation function between RTGS systems that have disparate pre-funding requirements.



ICN's Security Framework extends bank functions:

Customers send and receive funds via any method with unified accounting. Furthermore, customers will have the ability to transfer and receive any type of document where digital signatures are required to be validated with proven authenticity.

Motivation, a FED Faster Payment's perspective:

"In today's banking, payment, healthcare, and other systems we have a national identity schema that is based on a data-consistency model. This is not a legally-enforceable digitalized identity. It's just a good guess.

This is due to the conspicuous absence of successful open access protocols.

*We fill this gap by analyzing and understanding transactions over an identity's entire life cycle; we can risk-assess from onboarding to final settlement. We share what we learn in the form of a Gateway Protocol for inter-operability. So, as we proceed on this journey together, everyone has realistic expectations of what RTGS means. Anyone who is not telling you this is doing you, and themselves, a disservice."*⁶

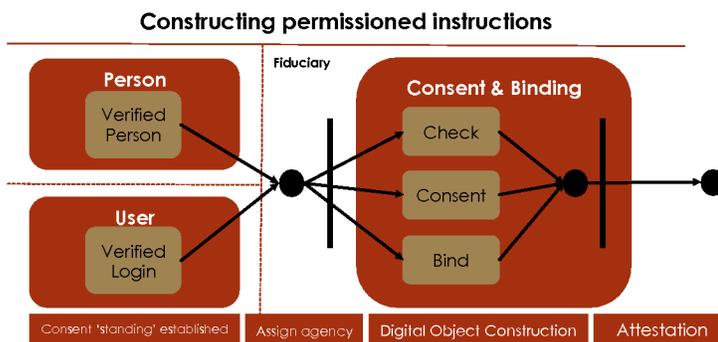
ICN advances the State of Play in the U.S. with a secure messaging framework that encapsulates every component of back and front-office services. This approach is as profound as it is flexible. Validation ledgers can be located wherever messages flow.

ICN's methodology re-structures messaging among financial applications enhancing security with differential access controls for lawful interception and audit reporting.

Optimization of secure messaging in business chains is done in a manner that covers risk with the level of certainty that ensures banks' profitability in e-finance and e-commerce real-time transactions.

Provenance construction

Trusted Context (with chain-of-custody for liable provenance)



⁶ Richard Parry – CEO Payment Pathways, Inc. and Principal – Parry Advisory, LLC Chicago, IL



This approach is timely because of it:

- Ensures fast implementations, superior cost-benefit ratios, and sufficient security and scalability, while avoiding costly maintenance, training, and support.
- Manages B2B eBanking policy compliance.
- Helps banks control internal and external administration costs.

About ICN:

ICN principals have specific payments project experience with a Top 25 Bank, a Fortune 250 global payment network, a Central Counter-Party (CCP) clearing organization, and inter-related International Standards Development Organizations (SDOs), including California's DMV, and securing dental patient data on ICN versus LANs and the web.

In the course of these projects, we have helped our Clients to develop advanced, sophisticated and functional banking, document management, security and supply chain finance applications (including patent applications), that support authoritative identity management service offerings.

Our approach advances the cyber-security marketplace to meet the API-economy requirements. The ICN design principle of ledger flexibility to validate liable provenance renders the protection of Web-centric attack surfaces as well as CCP entities moot.^{7,8,9}

ICN's T-Access markets

Product Tier	Application	Data Privacy Features	Prospects
Identity proofing Chain-of-custody instrumentation	C2B, C2b basic bill payments	~25 data fields e.g. Amount/due date, Account, Biller ID, Consumer ID, Bill ID, Bill cycle, Payment type, Digital signature, Payment Transaction ID, Address, Email,	Fiserv, FIS DMVs,
Insured access control Data life cycle management	B2b, B2b, C2b standard business invoices	~100 data fields e.g. Invoice identifier, Split Payments Custom breakdowns, Payment Validation Security & compliance, Payment Analysis Uncovering opportunities	Intuit Lending Tree, Angie's List
Real-time gross settlement Treasury management	B2B, b2B, C2B Faster stored-value transfers by vertical	~1000 data fields e.g. Shipping information, Split Payments Custom breakdowns, Payment Validation Security & compliance, Payment Analysis Uncovering opportunities, Cross Border Universal standard	Aetna, Amazon, Boeing, Ford Motor Co.

⁷ Why it works: <http://www.paymentpathways.com/wp-content/uploads/2018/12/2018DEC7-ICN-RTGS-Datasheet.pdf>

⁸ How it works: <http://www.paymentpathways.com/wp-content/uploads/2018/12/2018DEC14-ICN-RTGS-Use-Case-Rules-Flows-and-Mid-Level-Design-Specification.pdf>

⁹ State of Play ITU Focus Groups: <http://www.paymentpathways.com/wp-content/uploads/2018/12/2018DEC14-FG-Digital-Ledger-Technology-FG-Digital-Fiat-Currency.pdf>



The automation of knowledge-based decision-making requires financial outcomes that are not only precise but accurate with 100% certainty. Bringing such a level of certainty to FI, Enterprise, and Public mission-critical applications is unprecedented and long overdue.

Leveraging the strategic strengths and challenges of Community and Regional banks advances this strategic initiative through practical pilot experiences. A case in point, the U.S. perspective has traditionally been narrowly focused on what regulators would allow. The absence of American legislative leadership in PSD2, eIDAS, and GDPR legislative matters exposes why the State of Play in the U.S. is far behind. If problems didn't exist, there would not have been the need for legislation to mediate harms. Looked at another way, if ICN usage commonly protected important information transactions, problems would have been circumvented by design in first place.

Applicable law and compliance for data protection in RTGS:

The organizing principle of Open Access in Faster Payments is partially met by same-day ACH. True Real-time 24x365 Faster Payments, for this discussion – RTGS has been impractical for smaller banks without direct access to RTP-TCH. There is a palpable fear among bankers that Fintech solutions from unregulated entities might siphon off customers, weakening their institutions as customers follow their money flows, withdrawing deposits in the process.

Regarding Fintech solutions in the Digital Ledger Technology (DLT) space, we currently see a trend of stricter application of existing laws and drafting of new legislation that is focused on providing legal certainty regarding the validity and regulation of DLT transactions. We expect this trend to continue. By trying to comply, the industry is moving away from disruptive, but possibly non-compliant processes. ICOs converge with IPOs. Security Token Offerings (STOs) introduce central control.

Wall Street has led financial innovations since 2000. However, financial innovations usually involve high leverage and complexity. The 2008-09 financial crisis destroyed confidence in financial institutions.¹⁰ To save the financial system, boost confidence and recover the economy, the governments and central banks implemented aggressive monetary policies,¹¹ injected liquidity and tightened the regulations.¹² This stopped the economy from slowing down, but the action also brought back inflation and currency depreciation concerns.

¹⁰ John C. Bogle (2008), Commentary: Why we lost faith in Wall Street – and what to do, CNN <http://www.cnn.com/2008/POLITICS/12/01/bogle.investors/index.html>

¹¹ Ivana Kottasova (2016), \$9 trillion and counting: How central banks are still flooding the world with money, CNN, <http://money.cnn.com/2016/09/08/news/economy/central-banks-printed-nine-trillion/index.html>

¹² Governor Daniel K. Tarullo (2016), Financial Regulation Since the Crisis, <https://www.federalreserve.gov/newsevents/speech/tarullo20161202a.htm>



Quickly, Europe implemented the MIFID2¹³, and the United States implemented Dodd-Frank and re-spun Volcker rules¹⁴ to regulate the financial institutions, especially for Over-the-Counter (OTC) transactions. This came with a very high regulation cost and restricted innovation. Small financial institutions found it difficult to compete with the big ones. This further increased the degree of “centralization,” and financial institutions were regarded as “too big to fail.”

Currently, we see that legal innovation continues to lag behind technological innovation. However, at some point legal innovation will catch up and technological innovation will need to become compliant *by design*. It's time for regulators to again support smaller financial institutions.

The FED's role in NACHA's Federated Directory / DLT project:

ITU's Focus Groups (FG) developing standards in concert with ISO's TC-307 are:

- a. FG – Distributed Ledger Technology (FG-DLT); and
- b. FG – Digital Fiat Currency (FG-DFC).

ICN is an active participant in both Focus Groups. The NACHA-led, TBD-governed, Federated Registry system that was publicly announced at AFP-2018 can qualify as an illustrative Use Case for Legal Entity Identifiers for Micro, Small, Medium, and Enterprise (MSME) Businesses.

ICN is working with the FG-DFC to standardize the Gateway Protocol for securing Data Exchanges among the B2B registries that support RTGS systems, globally. The Global Legal Entity Identifier Foundation (GLEIF), endorsed by G20, is the main global implementer of the Legal Entity Identifier (LEI). Their web site is <https://www.gleif.org/>. It is ICN's position that its RTGS Ledger be federated and interoperable with [Global LEI registry](#). It would be highly desirable for the FED to express its strong encouragement that NACHA elect to conform to relevant ISO LEI naming standards.

Furthermore, it is a strong opinion of ICN that the FED should articulate its support that RTGS systems adopt rules designed to enable interoperation with SWIFT's validation directory (which is affiliated with GLEI) and other RTGS efforts such as RTP from TCH.

For example, besides a standard a way to resolve the business identification itself, a way is needed for a business entity to prove that he or she is really the owner of that attribute using a fiduciary's validation.

¹³ Philip Stafford (2018), Mifid II and dark pools: what are regulators up to?

<https://www.ft.com/content/491bfa8-f3ba-11e7-8715-e94187b3017e>

¹⁴ Volcker Rule, https://en.wikipedia.org/wiki/Volcker_Rule, Wikipedia as of Dec. 10, 2018



This could be done by a.) A centralized authority validation; b.) by a set of authorities who are 'federated' (verifiably trustworthy by rules) to do that, or by c.) a decentralized 'pocket registry' as 10 million enterprise users utilize every day.

1. Spotlighting a way forward, as an example of a centralized authority, Brazil has an existing public key infrastructure that performs the LEI validation function without manual verification. Brazil is developing technology to validate the digital certificate using a smart contract and automatically assure that the link is valid.

Relevant standards include:

- ISO 24760 defines an identity management system as user-focused "when it allows the individuals to play an active role in the management of the identity information stored in the identity register."
- A Legal Entity Identifier (LEI) is defined in the ISO 17442¹⁵ standard as a "20-digit, alpha-numeric code" that uniquely identifies "legal entities participating in financial transactions."¹⁶

These are just two of many 'stovepipe' approaches to standards. This piecemeal approach may hamper rather than facilitate selective disclosures for one to have sufficient control over the identity and trade data necessary to restrict data access/retrieval by unauthorized third-parties.

2. ICN is expanding its business base to include the Financial Industry, leveraging its insured 'BusinessChain Framework' for securing *trusted* access (e.g., *tAccess™*).

The use of a neutrally positioned Messaging security framework means using a functional digital ID that grows and lives beyond a life of a single program, intervention, or technology provider.

In summation, connecting fiduciaries as ID providers is consistent with NACHA's recently announced "B2B Federated Registries-on-blockchain" project.

¹⁵ ISO 17442. (2012). Financial services – Legal Entity Identifier (LEI). <https://www.iso.org/standard/59771.html>

¹⁶ GLEIF. (2018). Introducing the Legal Entity Identifier (LEI). <https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei#>