



FOUNDED 1890

2015 WASHTENAW AVENUE • ANN ARBOR, MI 48104 • PHONE (734) 741-5858 • FAX (734) 741-5859

- E-Mail: information@university-bank.com
- Web Site: <http://www.university-bank.com>

November 7, 2019

Via Electronic Submission

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

Re: Docket No. OP-1670, Federal Reserve Actions to Support Interbank Settlement of Faster Payments

Dear Ms. Misback:

University Bank¹ is pleased to comment on the Federal Reserve Actions to Support Interbank Settlement of Faster Payments, Request for Comments.

1. University Bank supports building both “(i) an interbank 24x7x365 RTGS service with integrated clearing functionality to support faster payments and (ii) a liquidity management tool that would enable transfers between accounts held at the Reserve Banks on a 24x7x365 basis to support services for real-time interbank settlement of faster payments.

(i) However to make the RTGS service a social and commercial success, the following items must be addressed:

A. The FedNow real-time payment system must conform to the Effectiveness Criteria established by the Federal Reserve’s Faster Payments Task Force² at the level of “Very Effective”.

1) The FedNow service should differentiate itself in the marketplace by strictly adhering to the security criteria for real-time payments which were noted as requirements by the Fed’s

¹ Founded in 1890, University Bank® is the 15th oldest bank headquartered in Michigan. We are proud to have been selected as the "Community Bankers of the Year" by both American Banker magazine and the American Bankers Association and as the second fastest growing business of any type in the Greater Detroit Region by Crain’s Detroit Business. As of 9/30/2019, University Bank was managing over \$24 billion in financial assets for over 137,000 customers and our 473 employees make us the 5th largest bank based in Michigan. University Bank is a state chartered community bank, with on balance sheet assets totaling approximately \$383 Million. We operate one branch office in Ann Arbor Michigan.

² The security effectiveness criteria are listed on pages 16 to 23 of <https://fedpaymentsimprovement.org/wp-content/uploads/fptf-payment-criteria.pdf>.

Secure Payments Task Force, to ensure that fraud is greatly reduced in the new real-time payment system. One key criteria that cannot be compromised is that data should be encrypted at all times: at motion and at rest. Data should never be unencrypted and in the clear. This is a key failing of the Zelle and TCH RTP payment ecosystems. **If the FedNow service strictly adheres to the security criteria for real-time payments at the level of “Very Effective” it will see much more rapid adoption and commercial success in the marketplace.**

If the FedNow payment system meets those security criteria at a “Very Effective” level, it will produce many positive benefits to society, including the elimination of the identity theft criminal ecosystem. According to a United States Department of Justice study, in 2012 the direct and indirect cost of identity theft was estimated to be responsible for financial losses of \$24.7 billion [emphasis added], approximately twice the \$14 billion total cost of other property crimes.”³ The cost of identity theft has risen sharply since then as major security breaches have occurred impacting nearly every American, and will continue to rise sharply in the future as the ubiquity of stolen personal information has reached critical mass. Nearly any information about any U.S. citizen can be purchased on the black market at a nominal cost.

2) “Envelope Security” and “Digital Rights Management” security should be employed to enable tight control of access to data in the FedNow system based on Role, Authority, Need to Know, Authenticated Status and Strong Enrollment. **It is probably impossible to meet all the security related criteria of the Effectiveness Criteria established by the Federal Reserve’s Faster Payments Task Force at the level of “Very Effective”, without using “Envelope Security” and “Digital Rights Management” architectures. Using these security methodologies will substantially enhance the privacy of every member of U.S. society and dramatically lower the incidence of identity theft.**

I was an active member of both the Federal Reserve’s Faster Payments Task Force and the Federal Reserve’s Secure Payments Task Force. I participated in nearly every committee of both Task Forces and served on the Steering Committee of the Secure Payments Task Force for its entire existence. I was privy to all of the discussions held by the Small FIs when they met as a group to discuss strategy. For strategic reasons, during the life of the Task Force the Small FI Segment opted not to ask the Federal Reserve for certain things, however I can attest from being an active participant in both Task Forces and a leader of the Small FI Segment Steering Committee of the other, that:

B. There is wide consensus among the community banks that participated in the Federal Reserve’s Faster Payments Task Force and the Federal Reserve’s Secure Payments Task Force that the Fed should adopt and/or enforce through regulation and/or via its direct action the following business principles:

1) Interoperability without adherence to high minimum security criteria for real-time payments which were noted as requirements by the Fed’s Secure Payments Task Force is dangerous and just leads to inferior services like RTP and Zelle, which have high fraud loss rates⁴ becoming

³ https://en.wikipedia.org/wiki/Identity_theft_in_the_United_States

⁴ Per the Fed study, “Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study” (see:

ubiquitous and foisting a new additional major increase in fraud on community banks and credit unions. **Interoperability with a real-time payment service that does not adhere to the “Very Effective” level of security criteria for real-time payments which were noted as requirements by the Fed’s Secure Payments Task Force should not be mandatory for FedNow or its FI customers.**

If the FedNow service meets the security related Effectiveness Criteria at a “Very Effective” level and any interoperable real-time payment systems are also required to meet the security related Effectiveness Criteria at a “Very Effective” level, then small FIs would support the Fed imposing a mandate on all FIs to use real-time payments and to mandate the receipt of any real-time payments by every FI, as long as those payments were credit push, or if initiated by merchants, authorized by strongly authenticated and strongly enrolled end users in conformance with a level of “Very Effective” for security related Effectiveness Criteria.

2) Because ubiquity is critical for adoption of real-time payments, and achieving ubiquity requires knowing to which bank to send a payment, **the Fed should provide a directory that enables users to securely query and determine the correct bank to credit to transact with for any person or business located in the U.S. using real-time payments. This Fed run system could be a node in a federated system with other directories, however the Fed’s role is critical, to ensure that small financial institutions are not disadvantaged by being charged higher fees for access to value-added services built on top of payment directory services owned by larger banks and large vendors.** Big data based services, such as the payment directories, inherently favor large scale enterprise, placing smaller financial institutions at disadvantages based on their economies of scale. Therefore a Fed role to ensure a level playing field in payment directory services is critical.

3) The economic case for real-time payments is better than just the business case outlined by the Fed, as there are many new value added services that would be enabled by real-time payment products. These would also provide economic incentives for FIs to participate in real-time payments. There are a lot of additional business use cases that will be enabled by real-time payments that we cannot even conceptualize today.⁵

<https://www.federalreserve.gov/newsevents/pressreleases/other20181016a.htm>), “the value of noncash payments fraud rose 37 percent from \$6.1 billion in 2012 to \$8.3 billion in 2015.” If this trend continued at the same rate, fraud would be \$11.4 billion in 2018. Zelle and the Clearing House RTP system are just real-time versions of ACH payments, with no new material security enhancements. By making ACH type payment real-time and irrevocable, they just accelerate the fraud ecosystem. As a result, fraud losses from Zelle are 5 to 6 basis points, while the Fed study indicates that fraud losses on electronic payments overall in the U.S. are 0.46 basis points. (see: “How Zelle, banks combat real-time payment fraud”, *American Banker*, by Penny Crosman, <https://www.americanbanker.com/news/how-zelle-banks-combat-real-time-payment-fraud>). If everyone switched all electronic payments to a Zelle/RTP type service, U.S. electronic payment fraud losses would increase at least 11x to \$123.5 billion.

⁵ University Bank itself detailed six of these value added services in its own submission that was vetted by the Federal Reserve’s Faster Payments Task Force RFP process. These use cases would create over \$30 billion in value⁵:

1. First Class Email
2. Cross-border trade facilitation services using a Single Window
3. Single Sign On Authentication and Credit Bureau services

4) Small FIs do not believe that it is too late for the Fed to introduce a real-time payment product to the market. The market demand is not yet very loud. We need to look at having a solution up and running, even if it's an interim solution that is later made more robust, so we can move ahead before the demand from the market gets too loud. Market demand is seen especially in the market enthusiasm around cryptocurrency based payments despite their serious flaws. If the Federal Reserve moves forward to build a new real-time payment system together with 24/7/365 RTGS settlement and liquidity services FIs could deploy to the market a superior solution that would quickly gain widespread market adoption. **The Federal Reserve should move forward as fast as possible in building these services without compromising on the required Security Related Effectiveness Criteria.**

5) Small FIs do not all have the resources to build necessary components to successfully deploy FedNow into the marketplace. **To ease adoption for all Small FIs, University Bank believes that the Fed should build and offer to all FIs FedNow based end-user services in the form of user interfaces for Apps for mobile devices and Web Services for PC based customers that leverage the FedNow capabilities. These FedNow based end-user interfaces should be able to be easily white labeled so that the branding of the FI is presented to the end-user.**

6) **University Bank has already built in Unified Modeling Language (UML) all the necessary components including all use cases and optional use cases for both consumer, SME and business end-user services requirements for a FedNow service. University Bank is willing to sell this intellectual property to the Fed at its cost of \$1 million and believes that this work could reduce the FedNow time to market by at least six months and materially increase the speed of Small FI adoption.**

7) **The Federal Government should get behind the FedNow real-time payment product the same way that it did to catalyze the creation of the ACH payment system and getting it to achieve critical mass. The Treasury should use FedNow exclusively for its payments, as should the rest of the Federal Government.** For example, social security payments and emergency disaster relief payments should be sent through the Fed's FedNow real-time payment system. This should be a mandate in rules, just as was done at the beginning of ACH. Mandates to make it required will reduce cost and creates critical mass and volume.

8) **We believe that the Federal Reserve should establish a mission statement and define a success statement, which its efforts in this area should be targeted to achieving.**

-
4. Healthcare payments & health information exchange automation
 5. Providing low cost financial services to the Unbanked
 6. Replacement for SWIFT

University Bank's proposed payment system, PayThat is highly secure and meets the security Effectiveness Criteria. University Bank's proposed payment system was one of the most highly rated proposals that went through the Faster Payments RFP process. PayThat is already architected in UML and could be built in about six months. University Bank stands ready to license or sell its intellectual property to the Federal Reserve to accelerate its process of rolling out a real-time payment system that conforms to the security requirements of the Effectiveness Criteria. For details of the six use cases and the details of the proposals themselves, please see <http://www.university-bank.com/paythat/>.

We suggest the following Federal Reserve Faster Payments Success Statement:

We would be successful if we architect and build FedNow as a payment system where all users are strongly enrolled, where all data is encrypted end to end at all times and never in the clear, in motion and at rest, and all access to data is tightly controlled based on authentication, role, authority and a need to know. We will achieve this if we strictly adhere to the security criteria for real-time payments which were noted as requirements by the Fed's Secure Payments Task Force.

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

9) To lower the incidence of fraud, to identify greater amounts of malicious activity more timely, and to lower the cost to FIs of compliance with BSA and AML regulations, the Federal Reserve should require banks and credit unions to join and form a new industry owned utility covering all payment systems, the Identity Credit Bureau.⁶

Identity Credit Bureau would create a repository and independent back office platform that could receive transaction and pending loan data from the participating banks and analyze and post back to each bank involved drafts of any required CTRs or SARs after the independent platform analyzed the data and recommended that a CTR or a SAR was appropriate to file. The bank's BSA Officer would then decide whether or not to file the CTRs and SARs and trigger the actual filing.

The pooling and examination of this mountain of data held by the Identity Credit Bureau could identify potential bad actors better than any individual bank could, since it would have a more complete picture of all transaction activity. The regulators (including FINCEN) would provide a limited safe harbor for such cooperation as long as the bank filed the draft CTRs and SARs suggested by the Identity Credit Bureau, particularly if the system was sophisticated and staffed by experts with high level security clearances able to gain access to confidential government databases.

Banks would save money by outsourcing their BSA work related to electronic payments, since currently each bank involved in a transaction must review both sides of each transaction. Therefore, centralizing the work will cut the cost of BSA compliance at least in half while doing a better and more comprehensive job. This could not only save money for banks, it could be a revenue creator for them as well since the Identity Credit Bureau after accumulating Know Your Customer Data on tens of millions of consumers and businesses could begin to serve as a banking industry owned credit bureau. The directory discussed above could be a by-product of the Identity

⁶ University Bank submitted a detailed proposal that was vetted through the Federal Reserve's Faster Payment Task Force RFP Process outlining the Identity Credit Bureau and how to accelerate adoption of this in the banking industry. For more information beyond this brief summary, see: <http://www.university-bank.com/wp-content/uploads/2017/07/Using-the-IAF-as-a-Catalyst-for-a-FI-Owned-Credit-Bureau-and-a-B2B-Directory-Use-Case-v1.pdf>

Credit Bureau at nominal extra cost. The value of the U.S. credit bureau industry, currently owned by non-banks, is \$17 billion. More importantly, the Identity Credit Bureau could protect participating banks from sanctions because an independent "utility" would make recommendations which the bank most likely would want to follow to gain the regulatory BSA/AML limited safe harbor.

10) If the Fed uses an "Envelope Security" based security architecture, it would be relatively easy and safe from a cyber security perspective to add a Fed issued Dollar Cryptocurrency to the FedNow service. We believe that this will be a national security imperative in the near future and not an optional task required of the Fed.

The Swedish Central Bank has outlined its plans to build and deploy a Euro Dollar denominated crypto currency based payment system. The Chinese Central Bank outlined its plans for a Renminbi based crypto currency based payment system which is to be deployed by 2024. The Russian Central Bank outlined its plans for a Rouble based crypto currency based payment system.

Elements of the U.S. Government have been analyzing these developments and have concluded that there is a potential substantial risk to the U.S. economy as a result, due to:

1. The severe limitations of SWIFT (it has no settlement capabilities, has network security design flaws and transactions with less developed nations take 7-10 days to settle frequently and might be bypassed), and
2. The widespread overseas adoption of Single Window systems to facilitate cross border trade in many countries overseas;

If a fiat currency based crypto payment system is available in Euro and Renminbi currency there is the possibility that there could be a rapid adoption of non U.S. Dollar based trade and under the worst case scenario this could lead to a catastrophic and rapid collapse of demand for U.S. Dollars used for foreign trade. That would cause a rapid & significant decline in the U.S. Dollar, high inflation and it could cause the collapse of the credit worthiness of the U.S. Government and the collapse of all the large banks regulated by the NY Federal Reserve Bank. While far from a certainty, due to improvements in third generation crypto currencies, it is possible that some of the limitations of first and second generation distributed ledger technology have been overcome and VISA Net type volumes at zero cost per transactions may be possible with third generation DTLs. Testing is required to validate these assertions which appear technically feasible.

As an insurance policy against the worst case scenario, we believe that the Federal Reserve should now participate in crafting a test and proof of concept in as non-controversial a way possible (and with low public visibility) so that it is prepared to roll-out a U.S. Dollar based crypto currency based payment system, or be prepared to approve the U.S. banking system doing so as safe and sound banking, before it is too late.

The U.S. could differentiate itself and gain a long term strategic advantage by leveraging its superior internet security and cryptography capabilities by building, testing and ultimately deploying a highly secure fiat crypto currency based real-time payment system leveraging envelope security technology.

ii) To make the liquidity management tool a success, the following items must be addressed:

1. Specific needs of Small FIs, Bankers Banks and Corporate Credit Unions will need to be accommodated.
2. Infrastructure will need to be updated.
3. Process flow will need to be reexamined.
4. Legal agreements and regulatory compliance will need to be updated.
5. Activity and velocity caps per FI will need to be implemented. The Small FI's account at the Fed will be open 24/7/365 and therefore overnight when their employees are not working. There would have to be a system of caps and thresholds for risk control, just as we use with our own customers.
6. To ensure fraud risk control due to the potential velocity of real-time payments, a second account at the Fed may be required to lower the risk to small FIs. If a second account at the Fed is required, excess balances should roll into interest bearing deposit accounts at the Fed. Small FIs should be able to use clearing balances. These account balances should count as reserves. If a second account at the Fed is required, we would need this account to have the same features as the master account.
7. Accounting structures will need to be modified.
8. Credit risks of community FIs, Bankers Banks and Corporate Credit Unions will need to be managed and monitored. How these risks are managed and monitored will be different for different community FIs, Bankers Banks and Corporate Credit Unions.
9. Small FIs are concerned that 24x7x365 operation that will be required for real-time payments is very difficult and expensive. Another party such as a Bankers Bank or Correspondent Bank should be allowed to stand in for the small FIs during non-business hours. We need to give small FIs options so that they don't have to do this work themselves.
10. Monitoring of real-time payment flows will need to be automated and monitored, especially for BSA/AML requirements.
11. The Fed should provide a lending option during off hours similar to daylight overdraft and its discount window borrowings to support off hours transactions, as well as during regular business hours. Small FIs already have collateral at the Fed to support these overdraft and lending facilities. The cost of these overdraft and lines of credit should be reasonable.
12. While processing of real-time transactions should be 24/7/365, the time of the final end of day for each daily transaction cycle needs to be set in the late afternoon or early evening. Small FIs generally don't have second shift or third shift employees.

2. University Bank is encouraged by the Fed's announcement that it intends to build FedNow, however many Small FIs believe that the Federal Reserve needs to engage in and fund R&D in the FinTech and Payments Space in general much more aggressively. It is a myth that private sector R&D has led the development of most innovative technology. In fact, government contracts and government sponsored R&D has been the key catalyst driving forward technological innovation for the past 500 years. The items funded could be established based on industry determined unmet needs established in consultation by a Federal Reserve run and funded Task Force similar to the Faster Payments Task Force and Secure Payments Task Force. No sustained

progress towards modernizing the U.S. electronic payment systems will be made without it.⁷ No new payment system has been introduced in the U.S. since ACH and that was only a success because the Fed and Treasury moved their transactions to the new ACH payment system to give it critical mass and volume. The U.S. Government is under investing in FinTech R&D and the Federal Reserve is the best placed agency to fill this absolutely necessary gap.

If you have any questions about the material presented in this comment letter, or require any assistance in implementing a program to create the services discussed, I am available to assist you in any way as follows:

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

Sincerely,



Stephen Lange Ranzini
President & CEO
University Bank*⁺ & University Bancorp, Inc.
Ann Arbor, MI USA

* Founded in 1890, University Bank[®] is the 15th oldest bank headquartered in Michigan. We are proud to have been selected as the "Community Bankers of the Year" by both American Banker magazine and the American Bankers Association and as the second fastest growing business of any type in the Greater Detroit Region by Crain's Detroit Business. As of 9/30/2019, University Bank was managing over \$24 billion in financial assets for over 138,000 customers and our 473 employees make us the 5th largest bank based in Michigan.

+ University Bank is a Member FDIC and an Equal Housing Lender. University Bank is a wholly-owned subsidiary of University Bancorp, which is listed on the OTCQB stock market under symbol UNIB. We are proud to be noted by American Banker newspaper as the:

- #3 top performing publicly traded bank in the U.S. in 2017 based on Average ROE;
- #1 top performing publicly traded bank in the U.S. in 2016 & 2015, based on Average ROE;
- #2 top performing publicly traded bank in the U.S. based over the period 2014 to 2012, based on Average ROE.

University Bank's five year average Return on Equity is 19.1%. University Bank's ten year annual average revenue growth was 32.5%.

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

⁷ University Bank corresponded with Federal Reserve Chairman Jerome H. Powell on February 9, 2018 on this topic. This letter and its appendices are attached to this letter as an endnote.



FOUNDED 1890

2015 WASHTENAW AVENUE • ANN ARBOR, MI 48104 • PHONE (734) 741-5858 • FAX (734) 741-5859
• E-Mail: information@university-bank.com
• Web Site: <http://www.university-bank.com>

February 9, 2018

The Honorable Jerome H. Powell, Chair
Board of Governors of the Federal Reserve
Federal Reserve Building
20th Street and Constitution Avenue
Washington, D.C. 20551

Dear Mr. Powell:

I wanted to share with you some observations about how the Federal Reserve could serve the nation more successfully in encouraging FinTech, and especially innovation in electronic payments, an area where the U.S. has unfortunately fallen behind several other more advanced countries around the world. If this problem could be solved, many benefits would accrue to our nation, including a faster rate of long term economic growth and job creation, a key priority of our national leaders.

I have enclosed a copy of the excellent book, How We Got Here, by Andy Kessler. I have also enclosed a three page brilliant essay entitled "The Irony of High Tech", a great read on the history of the iPhone and how the key technologies embedded in it was all funded by government R&D. I have shared copies of both this book and the essay with Todd Aadland, Gordon Werkema, Ken Montgomery, Jim Cunha, Susan Foley and Sean Rodriguez, as well as several key executives involved in the Fed's payment system innovation effort because I believe that the Fed needs to alter its strategy to succeed in its goals.

I have the privilege of serving as a founding member of the Steering Committee of the Federal Reserve's Secure Payments Task Force, served from inception on the Federal Reserve's Faster Payments Task Force and our bank submitted a highly rated detailed proposal for a new real-time, highly secure national payment system as part of the Faster Payments process. I've also served as a founding member of the Fed's Business Payments Coalition and as a founding member of the Fed's EBIDS project led by Mike Taipale of the Cleveland Fed.¹

The book and essay I've sent you lay out clearly that without government research and development and defense contracts, the computer revolution would not have occurred and smart

¹ I began working with the Fed's ePayments Strategy Office in 2000 and with senior executives involved in standards development, when I served on the ANSI X9 Board of Directors and represented the U.S. to the United Nations standard setting body for financial services, UN CEFACT TBG5 and the ISO global financial services standards setting body, ISO TC68. I lay this out so that you understand that I've been deeply involved in innovation in the financial services sector and worked with many Fed officials over my career.

phones would not exist today. I believe that the Fed needs to change its current hands-off philosophy regarding FinTech and establish an annual budget for research and development commensurate with the importance of FinTech in the U.S. economy and FinTech's potential to increase economic growth, innovation and high quality jobs.

Currently, eleven Federal agencies have a research and development budget of over \$100 million²:

- [Department of Agriculture](#)
- Department of Commerce - [National Institute of Standards and Technology](#)
- Department of Commerce - [National Oceanic and Atmospheric Administration](#)
- [Department of Defense](#)
- [Department of Education](#)
- [Department of Energy](#)
- [Department of Health and Human Services](#)
- [Department of Homeland Security](#)
- [Department of Transportation](#)
- [Environmental Protection Agency](#)
- [National Aeronautics and Space Administration](#)
- [National Science Foundation](#)

Each agency administers its own individual program within similar guidelines established by Congress. These agencies designate R&D specific priorities in their solicitations and accept proposals from the business and non-profit sectors. Awards are made on a competitive basis after proposal evaluation. In addition, the Small Business Administration runs the Small Business Innovation Research (SBIR) program, which is a highly competitive program that encourages domestic small businesses to engage in Federal Research/Research and Development that has the potential for commercialization. Through a competitive awards-based program, SBIR enables small businesses to address the specific unmet needs of the eleven Federal agencies listed above. Each year, these 11 Federal agencies designate R&D topics that are priorities for funding under the SBIR program and they are required to allocate 3.2% of their entire R&D budget to the small businesses via the SBIR program.

Why is the Department of Education or National Science Foundation meriting a government run and funded R&D program to address their unmet priorities for technology innovation and the financial sector is not meriting it?

For over twenty-nine years now as President & CEO of our banking entity, I've witnessed the social and political roadblocks to innovation in the financial sector first-hand. It is not in the interest of the largest U.S. banks to see true innovation in electronic payments, so they block every effort to do so. They currently have high market share of imperfect and fraud riddled legacy payment systems that were never designed for internet sourced payments and in fact should not be used for internet sourced payments.³ As a direct result the criminal ecosystem around identity theft

² See: <https://www.sbir.gov/about/about-sbir>; links to the various agency R&D programs are active on this web page.

³ See: "Legacy Bank Payment Systems and the Internet: A Toxic Cocktail", [American Banker](#), by Stephen Lange Ranzini, Sep. 11, 2014, <http://www.americanbanker.com/bankthink/legacy-bank-payment-systems-and-the-internet-a-toxic-cocktail-1069874-1.html#comments>

grows rapidly each year, much greater than the rate of economic growth⁴. A crisis point is coming as these trends are not tenable indefinitely.

The payment system infrastructure of the U.S. is outdated, not built for the purposes it is now being used for, therefore it is full of security holes and not advancing at the same pace as the global world leading countries. Underinvestment by the U.S. government in electronic payment systems needs to be reversed to foster more rapid innovation in the private sector. The attached infographic from The Clearing House showing the current status of global real-time payment systems, which shows how very far behind we really are. Why shouldn't the world leader in IT be the world leader in electronic real-time payments?

When the Secure Payments Task Force began and I was elected to the Steering Committee by my peers, I was asked by the Fed staff to define what success would be. I wrote:

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

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

The largest U.S. banks are now pushing into the market their "solution" for faster payments, which is just a sped up version of the current ACH system, a system based on the British faster payments system. All the flaws of the current ACH system are inherent in this solution, so it will accelerate the fraud and incentives for the criminal ecosystem to steal personal identity information. In fact, the Faster Payments Task Force and the Secure Payments Task Force established criteria for security required for a new real-time payment system, and despite McKinsey's blessing of it, the Clearing House RTP service does not actually meet the criteria as the security committee intended when it established them (I was an active member of the committee that drafted and approved the security criteria for the Faster Payments Task Force), because we mandated end-to-end encryption of all data in motion and at rest, and while the TCH RTP's data is secure *once inside* the new payment system, it is not secure at various points in the lifecycle of each payment, between the consumer and their bank, before it gets to The Clearing House RTP solution.

Many of the problems that need to be solved are long standing (for over two decades now) and in my opinion, impossible for the private sector to fix on their own. For example, federated identity

⁴ Some 16.7 million U.S. consumers had their identities compromised in 2017, resulting in \$16.8 billion in losses, according to consulting firm Javelin Strategy & Research. The number of people affected was up 8% from 2016 and was the highest ever. In addition, most of the 145.5 million consumers affected by the Equifax breach had their social-security numbers compromised, which will lead to accelerating future fraud losses. See: <https://www.wsj.com/articles/identity-fraud-hits-record-number-of-people-1517922001>

management must be ubiquitous⁵, yet the NIST NSTIC effort which I helped advise at inception has no traction in the financial services sector. Many solutions require critical mass (Metcalf's Law, i.e. the "network effect"⁶), and how can a start-up achieve this especially when the largest banks refuse to engage to protect their narrow commercial interests?

Government contracts and government R&D are essential and not optional in solving these problems. For example, the ACH system would never have gained critical mass in the U.S. if not for the Fed and the Treasury working together to move Social Security Payments to the new payment system.

The myth that the private sector leads innovation is just that, and I urge you to take the time to read the book and essay I've provided to you, so that you can understand first-hand, how this myth is damaging our country. The hunger for a real-time payment system in the U.S. is real, just witness the fact that a flawed technology such as Bitcoin could have a value greater at its peak than all but 15 of the world's largest publicly traded firms. Yet what the world needs is that the Fed leads the private sector through contracts and R&D to architect and build a new payment system with the success criteria I've outlined above. To get there, many specific problems must first be addressed successfully.

The Secure Payments Task Force can play a key role in assisting the Fed to set the research and development priorities, and annually allocate based on these priorities, funds from the Fed's research and development budget. The Secure Payments Task Force could designate R&D topics, create solicitations and accept and help vet proposals from the business and non-profit sectors. Awards would be made on a competitive basis after proposal evaluation.

Several hundred million dollars a year would materially accelerate the pace of change and increase the long term growth rate of the U.S. economy. However, even small amounts of money can make a key difference in the right hands. As one of our bank holding company directors once pointed out to me:

Just remember when Ernest Lawrence built the first cyclotron for the "Manhattan Project". Westinghouse and DuPont wanted \$20 million dollars and Ernest was so PO'ed by the price, he declared he could build one for less than \$500. He did and then bought some land in Livermore, California and started his own lab for the government named "Lawrence Livermore"!

In our bank's submission to the Fed's Faster Payments Task Force RFP, we outlined four business models that can create over \$30 billion in value from new activity not possible with the current legacy payment systems or TCH RTP system⁷. This is but one example of the untapped potential that the current social and political dynamics block. Solving this problem would strengthen both

⁵ See: "84 percent of businesses could reduce fraud risk if certain about customers' identity", January 24, 2018, <https://finance.yahoo.com/news/84-percent-businesses-could-reduce-143000836.html>.

⁶ A network's value is proportional to the square of the number of connected users of the system (n^2), or the number of functions supported by the network (f^2).

⁷ See: <http://www.university-bank.com/paythat/>. The four business models are: "First Class Email", "Cross-border Trade Facilitation Services Using a Single Window", "Single Sign On Authentication and Credit Bureau Services", and "Healthcare Payments & Health Information Exchange Automation".

the largest banks and community banks, grow our U.S. economy, create many new jobs, reduce fraud and potentially if correctly done, eliminate the identity theft criminal ecosystem. Isn't this a laudable goal that the Federal Reserve should back with an annual budget and a well thought out program?

As the Fed's new chair, you have the ability to change the Fed's long standing policy and obtain for our country and its citizens the many benefits I've outlined above. If I can be of any assistance to you in this regard, please don't hesitate to contact me:

☎ (+1)(734) 741-5858 xt 9226 [desk]

☎ (+1)(313) 408-8965 [cell]

☎ (+1)(734) 741-5859 [fax]

✉ ranzini@university-bank.com [email]

Best wishes,



Stephen Lange Ranzini

President & CEO

University Bank* & University Bancorp**

* Founded in 1890, University Bank® is the 15th oldest bank headquartered in Michigan. We are proud to have been selected as the "Community Bankers of the Year" by both American Banker magazine and the American Bankers Association and as the second fastest growing business of any type in the Greater Detroit Region by Crain's Detroit Business. As of 12/31/2017, University Bank was managing over \$20.8 billion in financial assets for over 120,000 customers and our 401 employees make us the 5th largest bank based in Michigan.

** University Bank is a Member FDIC and an Equal Housing Lender. University Bank is a wholly-owned subsidiary of University Bancorp, which is listed on the OTCQB stock market under symbol UNIB. We are proud to be noted by American Banker newspaper as the top performing publicly traded bank in the entire United States in 2016 & 2015, based on our return on average equity of 25.25% and 25.21%, respectively. We were also the second highest performing publicly traded community bank in the U.S. based on our 18.75% annual average Return on Equity over the period 2012 to 2014, according to American Banker newspaper. University Bank's five year average Return on Equity is 18.8% and our Return on Equity over the trailing twelve months to 9/30/2017 was 25.3%. For the past 5 years University Bank's annual revenue grew an average of 33.0% and our revenue growth in the first nine months of 2017 was 29.1%.

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

June 19, 2017

The Irony of High Tech

Technology is a major foundation of national power. Its uses are obvious. But the path from innovation to obsolescence is frequently less obvious.

Technologies that define an era usually come from a major geopolitical power. Roman engineering, for example, helped shape the Mediterranean world. British technology created and sustained the industrial revolution. These empires could absorb the cost of innovation because they had the money to do so and because they knew it would only reinforce their power. And because technologies are meant to reinforce power, even the most benign were invented for military purposes.

The Origins of the iPhone

Consider the iPhone, an invention of Apple, the genius of Steve Jobs, and a helpful, hip, and harmless product. Or so it would seem.

The centerpiece of the iPhone, as is the case with so many electronics today, is the microprocessor. The microprocessor was the fruit of the labor of a variety of scientists and engineers who were sponsored by the US government, which needed a lightweight computer for missiles, aircraft, and other systems. The technology quickly found use in the F-14 fighter aircraft, intercontinental ballistic missiles, and submarine-launched nuclear missiles.

Fast forward to 1985. General Dynamics, known at the time as GTE, helped the US Army create an advanced network for a device invented some 12 years earlier. The device was the cellphone, which would face its first true test in Operation Desert Storm. The Army needed a reliable wireless communications system that could be easily deployed, and the cellphone fit the bill.

Many of the iPhone's accessories and ancillary functions were developed for similar purposes. The idea of digital photography was developed by the National Reconnaissance Office, which needed a better way to produce photographs taken by their satellites. (Chemical photography

required developing, and that meant that the film had to be ejected by the satellite and caught by an aircraft in the air.) The NRO, therefore, developed a digital camera that could stream pictures back to earth. The descendants of this camera—this tool of spycraft—are found in every iPhone.

Maps and location services—a fixture on every iPhone—likewise have military forebears. GPS was originally meant to accurately guide the systems and vehicles of the armed forces, not Uber drivers. The satellites that make GPS possible, even today, are operated by the US Air Force.

And then there is the Internet, which is available literally at our fingertips. It was developed by the Defense Advanced Research Projects Agency, more commonly known as DARPA.

The more recent generations of iPhones, meanwhile, feature voice recognition software. SIRI, as we've come to know her, was originally a DARPA-funded project of SRI International, an American research institute.

The Mature and the Obsolete

A few points follow. The first and most obvious is that the iPhone, an icon of innovation, is actually a composite of older technologies; only SIRI was invented this century. To its credit, Apple updated those technologies, fused them into a single platform, and turned that platform into a brilliantly packaged and marketed product. Still, what is called “high tech” is frequently an older innovation updated for modern use. It's evolutionary, but it isn't revolutionary.

Second, the military is a primary source of innovation in our society. The 50 or so years the Cold War was fought, for example, was a heyday of technological growth. The technology needed to support global war—in space, in the air, on the sea, under the sea, and on land—required unbound creativity. In this regard, the United States, with its intellectual and financial resources, had the advantage. But the public is either unaware of or indifferent to the fact that much of the technology we now consider peaceful was designed to allow the US to wage global thermonuclear war.

Third, we are reminded not just of the age of technologies but of their maturity. Maturity is different from obsolescence. The microprocessor cannot be considered cutting edge—it was put

to practical use before 1970. But neither can it be considered obsolete—it is still widely used. It has become a foundation of society even though it is no longer being radically innovated. The same could be said of the automobile and the internal combustion engine. It was incredibly useful and would be sold for more than a century, but the basic innovations were in place around 1970, and the industry mostly became about marketing thereafter. The microprocessor has a bright future, but its heroic days are behind it.

The greatest innovations follow this loose pattern: A handful of scientists create possibilities, which are later developed for military use before being sold in consumer markets. Governments, which are responsible for national defense, typically underwrite the research; private industry, which eventually benefits from it, is too risk averse. Put differently, the private sector builds off the foundation created by the government.

As well the government should underwrite this research: New generations of technology are needed to raise productivity. If the model that has been in place since before World War II continues, then another generation of entrepreneurs will take advantage of military research and development, deploy it, and announce how much they dislike government interference in their work. Selling products is important, but we need to understand the role that war plays in consumer products. For the pacifists who love technology, and the libertarians who love it at least as much, there is a deep irony at work.

George Friedman
Editor, *This Week in Geopolitics*