Questions for the Public

Preface

Five desired outcomes (from the Consulting Paper, emphasis added):

Desired outcome 1: Key **improvements for the future state of the payment system** have been collectively identified and embraced by payment participants, and material progress has been made in implementing them.

Desired outcome 2: **A ubiquitous electronic solution(s) for making retail payments exists that does not require the sender to know the bank account number of the recipient. Confirmation of good funds will be made at the initiation of the payment.**[11] **The sender and receiver will receive timely notification that the payment has been made. Funds will be debited from the payer and made available in near real time to the payee.**

Desired outcome 3: Over the long run, greater electronification and process improvements have **reduced t**he average end-to-end (societal**) costs of payment transactions** and resulted in **innovative payment services** that deliver improved value to consumers, businesses, and governments.

Desired outcome 4: **Consumers and businesses have better choice** in making convenient, cost-effective, and timely **cross-border payments** from and to the United States.

Desired outcome 5: The Federal Reserve Banks have collaborated, as appropriate, with the industry to **promote the security of the payment system from end-to-end** amid a rapidly evolving technology and threat environment. In addition, public confidence in the security of Federal Reserve financial services has remained high.

Gaps and Opportunities (from the Consulting Paper, emphasis added)

1. **Check writing persists** because checks have important attributes, including ubiquity and convenience, which are not well replicated by electronic alternatives for some transactions. Many receivers of checks prefer other forms of payment but exercise little control over the sender to request a preferred form of payment.

2. In a world where several other countries are moving to **ubiquitous near-real-time retail payment systems, the U.S. payment system does not have this capability**.[6] The U.S. payment system has begun to migrate incrementally toward faster payments primarily through private-sector innovation; but these innovations, when considered in total, have not resulted in a ubiquitous near-real-time system.

3. Most **recent payment innovations** have yet to gain significant market penetration and **are still limited-participation systems** where both sender and receiver must join. Legacy payment systems tend to be more ubiquitous, making them efficient and accessible for those who already maintain a transaction account with their bank (payers and payees of any transaction).

4. Some **features** that are d**esired** increasingly **by end users are generally lacking in many legacy payment systems**, such as

- A real-time validation process assuring the payee that the payer's account exists and it has enough funds or available credit to cover the payment;
- Assurance that a payment will not be returned or reversed;
- Timely notification to the payer and payee that the payment has been made;
- Near-real-time posting / availability of funds to both the payer's and payee's accounts; and
- Masked account details, eliminating the need for end users to disclose bank account information to each other. Payment cards and wire transfers possess some, but not all of these features; check and ACH payments generally lack these features.[7]

5. In general, **cross-border payments** from and to the United States are **slow, inconvenient, costly, and lack transparency** regarding fees and timing.

6. **Mobile devices have potential to transform wide ranging aspects of business and commerce, including the payment**. Digital wallet applications on mobile devices provide merchants with valuable information that can be leveraged for commercial purposes such as consumer-specific location information, transaction history, and other context-specific data.[8] With some digital wallet applications, the payment instrument is selected during the initial set-up phase and the payment takes place in the background thereafter, reducing the visibility and choice of payment instrument at the point of sale. Payment service providers are seeking to define their service offerings in this new world.

7. Businesses (especially large ones) have payment and accounting systems that are complex and costly to change, making it **difficult to achieve automated, straight-through processing** of invoices, payments, and remittance information.

8. **Consumer fears about payment security** sometimes inhibit adoption of electronic payments.[9]

Response

General

Q1. Are you in general agreement with the payment system gaps and opportunities identified above? Please explain, if desired.

Digital technology makes many improvements in many walks of life possible. But it also liberates manifestations of our society—such as the payments system—from a legacy of fortresses and silos built around what appears to be a declining value in the role of payments by traditional banks and their services. We now see a wave of new companies—from breathless startups to rich and fearless digital companies (e.g., Google, Apple, Amazon, Facebook)—that do not care about the structure and integrity of the payments system.

The waves of innovation now chipping away at the infrastructure of payments militates against old business models—for good, and perhaps for ill. Transactions settled in real-time, with good funds, by trusted institutions—with the same ubiquity, scalability, and integrity of today's payment rails—are a common quest and inevitable outcome of digital processing technology available in the current century. But American society is taking a meandering path, with

expensive detours, and we need a regulatory and technology roadmap to guide these innovations so that at the end of the day, we have a payments system that is not only *eff*icient, and spares wasteful investments in new models that undermine safety and soundness, but also *suf*ficient to meet our evolving needs for security, usability, and sustainability as a viable business.

i. What other gaps or opportunities not mention in the paper could be address to make improvements to the U.S. payment system?

With that said, four additional points should be addressed in this effort. We note that the recent Canadian Payments System Review and the current UK Payments Roadmap effort (led by the UK Payments Council, which is a reasonable and appealing model for the Fed's role going forward under this initiative) would be good references to follow in thinking about all the drivers that will make the emerging payment system work in the interests of *all* the stakeholders and members of the ecosystem. Fundamentally, the drivers in both of these efforts focused on harnessing the properties of digital technology. This is a critically important transition for financial institutions in this country, and needs the guidance and direction of the Fed—representing all of the stakeholders in the payments ecosystem—to ensure that the resources expended by the industry are appropriate for the intended result of transitioning all able banks and credit unions into the new faster, more efficient digital payments paradigm.

One top-of-mind driver for change is the current dysfunctionality of resource allocations and returns on investments that have surrounded and accompanied the struggling effort by the legacy payment system participants to perpetuate the magnetic-stripe/plastic card paradigm—including and especially the currently stymied move to chip-card based system (both EMV and NFC)—but also addressing Card Not Present/Online transacting, PCI, and Fraud/Risk Management. The dysfunction illustrates the worst effects of a laissez faire, 'free market' system where one faction (primarily the bankcard brands and their big issuers, but supported by acquiring processors and other participants that make a living in the business from high merchant discount fees) has had a disproportionate say in how payments are conducted in this country.

It is bad enough that the rest of the developed world generally regards the U.S. as a backwater of payments, being by far the last significant nation to begin deployment of chip-based technology. But worse, the growing uncertainties of how that deployment might proceed, the prospective major changes that can be expected in the near future, and the apparent desire of the brands to quickly move onto NFC—with which implementations of PayWave (Visa) and PayPass (MasterCard) possess proprietary advantages—have rendered the market in turmoil over whether to invest (if at all), with no obvious prospects of business case justification for either merchants or banks.

The resulting likelihood that members of the U.S. payments ecosystem will nevertheless eventually be pushed into investing tens of billions of dollars for what can only be termed as minimal benefits is described in detail in the attached Appendix A: The Challenges of EMV/NFC Adoption in the U.S. Suffice it to say

that banking and merchant and provider resources should not be wasted this way—nor can or should the integrity of payments be compromised with suboptimal deployment choices for it made by a handful of overly powerful members of the ecosystem. Every step they propose to make with respect to modernizing the card payments system appears designed solely to perpetuate their status quo—thereby yielding a chip-based system that is barely better than the existing mag-stripe system. This initiative should result—as an exemplar of the overall thinking of the entire payment system—in providing a regulatory and technological 'roadmap' that enables participants to choose the best security and interoperability options available, rather than simply being asked to pay billions for baby steps proposed by the brands.

Another additional key driver for change in the U.S. payments system is the reduced U.S. competitiveness globally as it falls behind other developed countries more focused on moving beyond the payments technology of the past century (e.g., from magnetic-stripe/plastic card credential processing onto chip-based, shared risk-management, and ID-based systems). This is particularly noticeable in B2B and small business payments venues, where more than half of all payments continue to be processed by paper checks. The problem escalates cross-border, where PayPal is the only reasonable alternative to complex, expensive wire and funds transfer systems, and the only company to benefit from the few innovations in international transacting so far (e.g., 90+% of IAT volumes on the ACH network are for PayPal transactions).

While SEPA (under the EU's Payment Systems Directive) has had its own complexities (and implementation challenges), the EU stands to become much more efficient in moving capital from country to country—and, potentially, fostering the Euro as even more of a replacement reserve currency for global commerce. U.S. companies attempting to expand into global markets can find themselves disadvantaged by inferior systems for paying, getting paid, and moving funds where (and when) they are most needed. This persistent and competitive need must be addressed with specific attention in this effort.

Another additional consideration is the vast challenge of reconciling—even rationalizing—the U.S. banking system with the societal tradeoffs between sustaining the costs physical assets and investing in digital infrastructure and capabilities. Can the U.S. continue to afford 100,000 branches and 14,400 regulated financial institutions—more than half of which issue credit and debit cards, and nearly all of which support ACH services? As all of us are learning with the Durbin Amendment impacts, many mostly smaller FIs do not have the cost structures to enable profitable debit card operations at the much lower rates that exist today (much less even lower rate prospects in the future…). Yet these smaller institutions continue to rate high with consumers and small businesses for trust and reliability—until the question of provision of mobile and digital services comes into play. It is simply not possible for many smaller banks and credit unions to make the investment in digital capabilities the way big banks can in order to leverage this trust.

This was clearly evidenced in the initial phase of mobile banking adoption. Many of the smaller FIs rely on a 'lifeline' from core service providers like FIS,

Fiserv and Jack Henry; but the lag-time in deploying comparable services enables the biggest banks to enjoy recurring advantages in adoption of new technology. And there is ample evidence (best seen in Alix Partners' recent survey report on the implications of mobile usage for banking) that digital and mobile users have a short fuse for getting the digital services they want—leading to high propensity to switch FIs.

A fourth additional consideration is the lack of real cooperation among industry participants *as a cohesive ecosystem* as exists in many other developed countries. One measure of the dysfunction of the U.S. payments system is the decades-long rancor that exists on bankcard pricing and rules, and enormous costs that these unending fights have on participants and in the public's perception of industry credibility. This animosity is not limited to credit and debit cards—though they are a major source of the problem; there is also contention with ACH network rules and rates—most notably the inability to meet the very high hurdle of a 75% majority needed for making a major change such as same-day settlement (the recent vote garnered an estimated 62% favorable vote from the NACHA voting community, but failed…). Clearly some open discussion needs to take place on how the long term strategic use of the ACH network meets with the needs of the entire payments ecosystem; such discussion should seek to achieve a balance between fair compensation for costs (such as proposed with the recent RDFI compensation for returns—also voted down) and opportunities for leveraging its unique attributes (very low costs with near-ubiquitous reach to 98% of FIs).

Q2. Are you in general agreement with the desired outcomes for payment system improvements over the next 10 years? Please explain, if desired.

The U.S. payments system is often (and increasingly) criticized on several dimensions (e.g., too credit card focused, too check-based, too expensive, too slow, too risk-prone, too-long resistant to smart cards, too insulated from other payment modes and types utilized in other parts of the world, etc.), but it has managed to host the world's largest economy (and its most fully manifested embodiment of free-market capitalism); and it accommodates a profuse array of financial institutions participating directly in multiple, global, bank-owned networks. The result has been provision of a core (albeit expensive) set of services that are generally perceived to be reliable and largely incursion-free. These services are financed both by direct fees (paid by merchants and corporates) and indirect charges (from consumer and client product fees)—which are built into a widely available set of product and service offerings by more than 14,000 banks and credit unions (and provide a substantial portion of their earnings and financial viability).

Credit and debit card interchange fees (until the recent impacts of Durbin) have historically been a primary and sustaining source of income that finances general operations for these banks and credit unions. For example, one credit union with $4 billion in assets (making it a top 20 ranking institution in that financial segment) generates 65% of its net income (which is distributed eventually to its many thousands of members) from interchange. (Because it has

fewer than $10 billion in assets, it is currently exempt from Durbin fee cuts). While a reduction in payment costs and risks (both funding and transactional) from this initiative would be welcome, if accompanied by a 'downdraft' in income from fees and charges (as has happened with non-Durbin-exempt institutions), the result on overall operations (and financial soundness) could be very disruptive.

Therefore, attaining the stated outcomes of this initiative needs to anticipate and guide the evolution of the payment system to a more efficient, digital mode—with appropriate mechanisms and timeframes to assure a practical and rational transition for those financial institutions that can figure out how to provide new value, and without sacrificing or risking the benefits that the system provides today. But banks should no longer expect—under the protective mantle of incubating regulation—that they are entitled to the revenues that they make today, in perpetuity for the future. Compensation to banks needs to be fair, in proportion to real and meaningful value-added, from today's declining mix of interest arbitration replaced by steadily rising fees. The opportunity to transition to new and different economic foundations for providing value to customers—including the opportunity to research, craft and build-out new digital revenue models—needs to become a key part of this migration plan to digital transacting.

Check 21 demonstrated that 'sea changes' in transitioning from physical to electronic forms of payments are possible. Check 21 was the result of enlightened leadership by the Fed to organize the payments ecosystem (and elicit Congressional support) to create laws to support and means to convert paper checks to electronically processed images. The result was ridding the system of tens of billions of paper checks per year that cost banks anywhere from $1-3 apiece. Yet 1/3 of the check volume—nearly 20 billion in all—remains with us.

There are options (e.g., EPO) to further tweak the electronic possibilities for remaining checks, but the problem with the 'long tail' of physical world products might have more to do with the failure of electronic alternatives deployed to-date to materially produce value *to users*—rather than just to providers. A good example of this is all the difficulties for paycheck-to-paycheck households who switched to electronic bill payment, only to find that current business models do not provide the needed flexibility to time (and delay) payments when erratic incomes (resulting from the *banking* crisis) can't support the automated 'rules' for auto-debit and auto-pay. The result is mounting fee charges imposed on them by both banks (and billers, like ATT, that hit overdrawn accounts 3-4 times). [This problem is explained further in the response to question #14.]

The proposed outcomes from this initiative need to address both bottom-line aspects of payments (costs) *and* top-line operations of every financial institution, taking into account the likely provision of competitive services from new providers that will undermine most if not all of today's banking revenue models. Such new entrants to the marketplace have the benefit today of reduced regulatory compliance requirements, for example, under the existing system, which provides them with a significant cost advantage vis-à-vis regulated

financial services providers. One well-debated example of this race to the lowest cost payments network is the proposed wider use of the ACH for broader consumer-based applications. Such uses would logically require investments in near-real-time authorization, authentication, creation of peering-level, independently-operated data centers, and more extensive transaction reporting and monitoring capabilities; but the current rate structure doesn't support compensation for those investments.

Achieving these outcomes would therefore call for both a definitive, protracted process identifying, understanding and managing these transitional aspects, tethered to a 'roadmap' (similar to what Canada has done and the UK is now doing) that assists the industry in reaching stable, reliable sustaining services within the stated 10-year timeframe without taking undue risks to the integrity of the evolving payments systems and infrastructure.

i. What other outcomes should be pursued?

Another key outcome of this initiative should be a comprehensive review of banking regulations that affect any and all aspects of digital transacting. The prevailing mode now is to simply try to adapt existing standards—e.g., Reg E for DDAs to new payment forms and modes, such as mobile payments, P2P, and real-time debit—all of which resolve transactions in near real time. Would a 60-day window for rejecting an ACH transaction be useful or necessary for such near-real-time transactions? If not, what *would* adequate user protections be (for both payers and payees)?

Another outcome might be to review the frequent disconnects among the regulatory agencies. For example, the CFPB's effort to create innovation 'laboratories' to cultivate better technologies for notifying and informing consumers about payment terms (e.g., fitting effective messaging and navigation to terms on small mobile device screens) sounds like a good idea, but it can also be viewed as a bit dysfunctional, when spawning requirements by other regulatory agencies for banks to vet the consultants and vendors they do business with become so extreme that only a few small, innovative companies can navigate the vetting process in order to work directly with banks? It would be a shame (and an industry disservice) to engineer the technology and business aspects of digital transacting for the future—while keeping the 'blanket' of 20th century regulatory interventions cloaked over the industry.

Q3. In what ways should the Federal Reserve Banks help improve the payment system as an operator, leader and/or catalyst?

The politics of payments in the U.S. has reached an ongoing crescendo, introducing many dysfunctions and unproductive additional costs. Many larger banks, for example, tend to be very leery of providing cost data (including risk management information that could be of benefit to the entire industry…) to the Fed out of fear that it might be used to foster further regulation—including reductions on fees levels and increases in fraud-mitigation responsibilities. As well, some of these big banks argue that excessive (and uncompensated)

'sharing' of best practices financed by individual participants (as one of the few means of achieving tangible competitive advantage in the marketplace) can discourage participants from investing in innovation.

On the other hand, the U.S. payments system has also incurred substantial criticism for being too dominated by a handful of big banks (e.g., the top five credit card issuers control 87% of the total spend, and the top 10 banks control 40-90% market share of nine other financial services) and the impact of such high levels of market concentration to society (e.g., the seemingly unending spate of lawsuits over payment card interchange, outrage over PCI requirements and costs, criticisms over the 'accepted' level of fraud, and all these unproductive costs on the industry). So there is pressure to re-think how the payments industry—with banks as primary providers—could or should be guided by some governmental body making sure all stakeholder interests are addressed.

One alternative proffered to an 'activist' Fed role is self-governance by the key industry participants. In the case of the big banks, the public perception that the they operate with substantial market power and self-aggrandizement is heightened by the immense number of disclosures of lawsuits and regulatory judgments flowing from the role of the big banks in the recent financial crisis. There is a growing chorus of concerns from all the smaller and mid-sized banks that their interests are not only being comprised by the agendas and actions of the bigger banks, and that they are being dragged into litigation and legislative battles that are not really their fights, but also that nominal industry self-regulatory groups and consortia (e.g., the credit card associations, NACHA) tend to be dominated—especially in terms of policies and future directions—by the bigger banks. One widely discussed example is last year's ACH member vote on moving to same-day settlement, which failed to achieve the high 75% approval rate needed; opposition to this initiative—which was supported by both NACHA itself, and the Fed—was led by the biggest bank ACH originators and recipients.

But in at least one case—The Clearing House's decision to pilot quick-response codes as secure payment tokens as a proposed industry standard (versus or as an augmentation to the problem-ridden NFC push by the card companies)—bigger banks have taken the marketplace lead instead of waiting for the industry consortia to act in a more responsive, market-focused way. (We note that in this case, Visa and MasterCard quickly introduced their own attempts at a tokenization standard, in collaboration with American Express). So there is no justification to *exclude* the bigger banks from a role in payments system improvements—just a need for more balance and harmonization with other interests.

Self-regulation per se does not seem to be a viable option at this juncture for perhaps a more obvious reason. A cursory review of the 10-Ks of the top five banks reveals dozens of legal and regulatory judgments *exceeding* $100 million apiece over the past five years. One top bank has incurred judgments of $29 billion, and legal fees of $23 billion in just the past year! Whatever concerns the big banks have these days, one of them is clearly *not* the efficacy of the payments system (which constitutes a huge source of their retail profits).

.

Another alternative to a proactive Fed leading the industry through the digital migration might be the creation of a new, formal body to manage payments. Few participants appear to have much appetite for investing in yet another organization (having just digested the formation of the CFPB) that not only would need a lot of support, training, and coordination, but also have the potential to *extend* the regulatory 'blanket' over the industry in one more new dimension. That is why part of this initiative needs to an effort to rationalize the types and amounts of regulation necessary for the digital realm—in effect, a 'zero-based budgeting' type of exercise (which might include coordination with other regulators such as the FTC and FCC, and certainly the CFPB).

Ultimately, the Fed—willing or not—is the logical (and perhaps only) entity that has sufficient experience, breadth, resources, and authority (explicit or implied) to assume the role of facilitator of a new payments system. The distinctions between the Fed as "operator," "leader," or "catalyst" seem somewhat artificial, then; it is all three.

Obviously the Fed continues as an operator (of the ACH, wires and other correspondent banking services, check handling, etc.) but is also an active participant (in many cases offering services to smaller institutions so that they can compete with bigger banks…). This role certainly qualifies the Fed as an experienced member of the payments ecosystem, but could produce some complications if/as it becomes the de facto, superordinate body functioning as the "leader" of the migration to a new payments system (or, in some scenarios, the creator and operator of a new, purpose-build digital network). And, by dint of this initiative, the Fed is already performing as a "catalyst" to push the U.S. payments ecosystem to more expeditious embracing of digital technology than existing participants—especially banks—have been able to muster to-date.

The Fed can—and must—serve in the "leader" role for this kind of effort, but should convene other parties to a supernumerary process that *proactively* solicit and adjudicate the contributions and interest of the entire payments ecosystem—including and especially digital and mobile providers. This faster payments initiative is a good start in that role.

The Fed's convening of a balanced, equitable ecosystem plan should logically also deal with a number of other structural challenges to the industry—such as patent threats (from trolls), frivolous class action lawsuits, conflicts in compliance and reporting requirements (especially across channels and borders), defining what a 'financial institution' is in a digital realm and what regulatory compliance applies, and how to move beyond existing impediments to creating and participating in collaborative efforts (including standards).

With respect to the latter challenge, we believer there is a growing consensus (although perhaps not among the biggest banks) to fashion a 'roadmap' of the minimum requirements for digital security and privacy so that payments providers can compete on the quality of their marketing and value propositions—not on their ability to capture and monetize transaction data. Without addressing both the structural impediments to innovation that have arisen over decades *and* the big new challenges (e.g., abuses of 'big data' and personal information), setting national policies for payments addressing only

tweaks in existing payment networks will simply shuffle around the same array of problems that exist today.

Ubiquitous near-real-time payments

Q4. In discussions with industry participants, some have stated that implementing a system for near-real-time payments with the features described in the second desired outcome (ubiquitous participation; sender doesn't need to know the bank account number of the recipient; confirmation of good funds is made at the initiation of the payment; sender and receiver receive timely notification that the payments has been made; funds debited from the payer and made available in near real time to the payee) will require coordinated action by a public authority or industry group. Others have stated that the current payment services are evolving toward this outcome and no special action by a public authority or industry group is required.

i. Which of these perspectives is more accurate, and why?

Real-time debit has existed in the form of EFT/ATM networks for decades, but it took start-up Dwolla and large bank core system provider FIS (with PayNet) to produce non-PIN-debit network versions of it. P2P services were introduced by PayPal (among others) more than a decade ago, but it took an entire decade before dozens of providers—including banks—were able to field relevant product offerings of their own. Mobile banking has been available since the early 2000s, but it took nearly a decade to get market penetration to a level of one-quarter of banks participating. Prepaid products—also pioneered from outside the industry (including merchant-issued, closed-loop offerings)—have evolved quickly with innovations by new industry participants (e.g., American Express with Serve and Bluebird, GreenDot, Incomm and others), creating a new category of product (prepaid debit cards) that appeals to the unbanked as well as those who do not trust or like doing business with banks. So banks are decidedly not in the forefront of payment innovation.

Probably the most illustrative example of the inability of current payments system and its primary participants—the banks—to expeditiously harness the power of digital technology is PayPal. In the first generation of eCommerce. PayPal began (as x.com in 1999) as a mobile payment platform, then morphed to P2P, then settled on lower-cost core payment processing for smaller online merchants. Once offered for sale to a top five bank for $75 million (in 2001), PayPal was purchased by eBay for $1.5 billion a year later, and now commands a nearly 20% share of online purchases. The top-five bank that rejected the initial proposed purchase believed it could build something better; it spent an estimated $225 million for its own P2P product, which was mothballed in less than two years when market adoption failed to materialize.

And the case of same-day settlement for ACH applies in this instance as well; big banks resist further market inroads by ACH to avoid risking cannibalization of their credit and debit cards. But today, when most FIs cannot make a profit on debit cards at the Fed's original $.21 cap rate—and will clearly lose money if the recent court rejection of the $.21 rate winds up cutting

interchange rates in half again (Judge Leon's court)—this argument has lost substance.

Further, the effort by the three biggest ACH banks to build their own P2P payment utility, ClearXchange, is already experiencing difficulties in working together, convincing smaller banks to trust them, and fielding a relevant digital product in an already crowded market. Banks simply are not good start-up innovators; at best, they can be fast followers (e.g., with online banking and bill payments); but even then, the innovations can stall out. Two examples illustrate the problem: online banking and bill payments, vis-à-vis biller direct models, and closed-loop merchant prepaid vs. bank open-loop cards. For nearly a decade, bank researchers have forecast that bank-provided offerings would eclipse both biller-direct volumes and closed-loop prepaid use, but that has still not happened, as users continue to find more value from more flexible and less fee-prone non-bank alternatives.

Finally, the U.S. is among a small handful of countries (and the only developed nation) to still not deploy chip-based card acceptance (i.e., EMV contact and contactless). Largely this is the vestige of bigger banks being unable to amass a business case justification for EMV (or NFC) themselves. But the market adoption problems are much greater for key users because of the way the card companies chose to implement them (i.e., card-emulation mode, which provides only baby steps in additional security at great deployment costs for merchants, and too many choices of cardholder verification methods—CVMs, making it difficult for issuers to field a low-cost card that works in more than a few countries cardholders travel to). [Please see Appendix A for more details.]

ii. What other perspective(s) should be considered?

Many in the industry believe that the ultimate solution for digital payments is to have a 'pipe' that allows high-level software-based mathematical cryptography to pass a generic 'cryptogram' representing value that is funded somewhere in a secure 'cloud' and accepted anywhere. This value is transferred—in electronic form—in near-real-time, as good funds, with substantial (though not complete) anonymity, and with an open, accessible ledger for each transaction. Around this pipe (which Bitcoin and other virtual currencies illustrate the viability of, in addition to both advantages and disadvantages…), a digital infrastructure must be created to ensure adequate security, usability and stability of the value tendered.

Bitcoin and the others do *not* provide that infrastructure yet, but it appears to be coming in the near future—given all the money being invested in this new sector. The Fed can learn from these experiments in virtual currencies about how to build the pipes for truly digital payments; but without guidance from the Fed as to what infrastructure is both necessary and adequate for integrity to the resulting payment system (e.g., fees that reflect *actual* costs and fair profits, compliance with anti-money-laundering requirements, etc.), virtual currencies are likely to pose both disruptions and risks to the existing system.

Q5. The second desired outcome articulates features that are desirable for a near-real-time payments system. They include:

a. Ubiquitous participation
b. Sender doesn't need to know the bank account number of the recipient
c. Confirmation of good funds is made at the initiation of the payment
d. Sender and receiver receive timely notification that the payment has been made
e. Funds debited from the payer and made available in near-real-time to the payee

i. Do you agree that these are important features of a U.S. near-real-time system? Please explain, if desired
ii. What other characteristics or features are important for a near-real-time system?

The Fed should convene both banking industry participants (i.e., card brands, bank networks, financial institutions, processors and regulators) *and* other critical participants in the payments ecosystem (e.g., merchants, corporates, consumer and business advocates, the CFPB, non-bank networks, and digital companies such as PayPal, Amazon, Apple, Google and Facebook, and even mobile carriers and application providers). It is of interest to note that the Fed has convened an informal version of this digital payments ecosystem with its Mobile Payments Industry Workgroup. MPIW has functioned for more than three years, hosting conversations unique in the industry for the breadth and candor, and fostering shared learnings of all the different—but essential—points of view of all the participants in a rapidly evolving business. Such sharing (unfettered by the potential that some market participants could suppress viewpoints—or policies—by their domination of the marketplace) would seem to be a vital objective motivating the move to a near-real-time payments paradigm.

It is also of significant interest to note that is no accident that many such national bodies that have preceded this initiative in other countries (such as the European Payments Council, the UK Payments Council in the U.K., the Finance Ministry in Canada, the Reserve Bank of Australia in that country, and similar models in other developed countries), and that they were convened first and foremost on the basis of addressing *national* issues and challenges in payments fraud as the primary motivation for collaboration. Efforts along these lines apparently have been proposed *within and by* certain Fed staff a number of times in the past decade, only to be rejected each time—apparently out of big-bank concerns that they would lose competitive advantages with respect to risk management innovations. Such a perspective (if accurate) makes no sense whatsoever in absolute terms, and makes even less sense in relative terms, given the 'radioactive' existence of the big banks, and their card brands, over the past decade or more.

Q6. Near-real-time payments with the features described in the second desired outcome could be provided several different ways, including, but not limited to:

a. Creating a separate wire transfer-like system for near real time payments that leverages the relevant processes, features, and

> infrastructure already established for existing wire transfer system. This option may require a new front-end mechanism or new rules that would provide near-teal-time confirmation of good funds and timely notification of payments to end users and their financial institutions.

The global movement to ISO 20022 represents (at long last) a fundamentally sound new paradigm for B2B money transfers and remittances, as well as automated invoice processing, general ledger updating, and expediting of order entry and inventory allocation functions. Payments are an essential component of corporate commerce, but do not drive the overall value proposition. So it will be important that any digital replacements for wire transfer payment functionality harmonize with the future of B2B transacting. And it will be useful to note the transition that smaller banks have been able to make in accessing correspondent banking services (e.g., wires, ACH, check images, etc.) via web services in ASP/SaaS configurations (from providers like Lending Tools): digital functionality works well in this mode, exhibiting the fundamental property of leveling the playing field for all forms of payments and related services among all banking participants.

But such changes that drive such obvious value from automation and lower costs to users also threatens a major source of (mostly) big-bank profits—from legacy wire transfer operations. This objection has surfaced in debates over the use of the low-cost ACH network to fill many of these funds transfer needs—including same-day settlement of ACH transactions. Such positioning seems illogical on its face *if* replacement services are at least as secure and efficient as the various wire transfer networks and systems. Innovation nearly always *removes* costs; why should that be any different for banking?

Furthermore, the banks' own electronic alternatives to physical wire transfers, such as account-to-account transfers via online banking, have not worked out well. A number of lawsuits have been waged against banks by commercial customers because the minimal security requirements for conducting online funds transfers *through and by the banks* have been vulnerable to malware attacks and compromises. Moreover, bank practices vary on how much of the funds transferred in what periods for electronic transfers. For example, it takes a top-five New York bank 3-5 business days to 'push' a recurring account-to-account funds transfer to a small credit union in Colorado, but that same credit union can 'pull' those funds (through an ACH debit) from the New York bank account in just 24 hours…. Does that make any sense?

Finally, it is immensely interesting to note how aggressively S.W.I.F.T.—the premier money transfer network in the world—is promoting digital innovation (e.g., in ISO 20022, mobile, etc.), and, in many respects, is 'dragging' its member banks along in the process (grudgingly, if not kicking and screaming). Such a posture by the leading practitioner in this business makes the argument for 'protecting vested interests' of incumbent wire transfer providers seem all the more vacuous and disappointing.

b. Linking together existing limited-participation networks so that a sender in one network could make a payment to a receiver in another network seamlessly. This option may require common standards and rules and a centralized directory for routing payments across networks.

There are discernible differences in what limited-participation/closed-loop networks bring to the party (e.g., easier account set up, faster throughput of money movements, streamlined use and integration into related transactional systems, and lower fees and costs for payers and payees alike), and what they do not. They often require both the payer and payee to have accounts within the network (in the case of P2P), to develop separate authorization, acceptance and settlement capabilities (in the case of alternative payments for POS), or deal with credit-granting and risk management on individual provider bases (in the case of private label products). Integrating these disparate networks and transaction systems is daunting, which accounts for the reluctance of many banks and merchants to invest in making the services available to their customers without some evidence of critical-mass penetration.

On the other hand, some 'hybrid' providers appear to able to provide the needed integration, when banks will not. Take the case of PayPal again (one of the industry's few major successes as an alternative payment provider), which relies upon highly manual processes for managing risk and resolving problems while riding the existing banking networks (and incurring lower costs and responsibilities than the banks do…). PayPal is the back-up provider for many P2P services (including those provided by banks and bank processors) for funds transfers that go outside the captive, closed-loop network. For such a service, where the funding typically moves to an email or mobile phone number account, PayPal typically receives revenue of about $.25 per transaction, while incurring few liabilities for the transaction itself. Banks could provide a similar service, and save themselves the $.25 fee—if they could manage their own interconnections to external networks.

American Express's Serve and Bluebird offerings (the latter provided in conjunction with Walmart) provide similar digital transaction management services—including the most commonly needed banking capabilities, such as bill payment and online purchasing—at fees far less than the rest of the prepaid 'card' industry. As currently configured, open-loop bank networks (other than the ACH) cannot begin to address such business model innovation and economics.

So, a move within 10 years to a 'universal' payment mode riding interchangeably among a multitude of open- and closed-loop networks seems a bit out of reach—at least for retail payments, and unless a new, purpose-built digital network comes into being. In any event, banks could certainly accommodate (and profit from) providing the digital identification services that these innovators offer—but on a more universal basis, across any transaction channel. For evidence of the viability of such a proposition, simply observe what the Canadian government has been doing with creating and fostering digital IDs for all the various electronic services users needs (besides payments): Voter registration, drivers' licenses, tax filings, hunting licenses, and so on. Such use

creates substantial value for users—value that can be monetized at a level that can eclipse what banks make in payment fees and charges.

c. Modifying the ACH to speed up settlement this option may require a new front-end mechanism or new network rules that would provide near-real-time confirmation of good funds and timely notification of payments to end users and their financial institutions. Payments would be settled periodically during the day.

The politics of ACH use notwithstanding, that network's ubiquity and 'industrial strength' support (from the Fed and EPN) make it an attractive choice for a default digital network. But the ACH processes transactions in complex formats in batch modes over 'borrowed' computing facilities, with clearing and settlement windows of typically 1-3 days. ACH formats are more than three decades old, rendering them very difficult to integrate into streamlined digital transacting systems. Returns are expensive to deal with, and fraud—especially account takeover fraud—is a rising threat. These aspects, then, make ACH a candidate for substantive rebuilding in order to fulfill that mission (i.e., real-time authorization, authentication mechanisms, linked clearing and settlement through dedicated peering centers, availability of good funds, etc.). The investment, time and effort required would be considerable, and not feasible without some basic change's in the network's policies for remuneration of participants.

It is conceivable, however, that the ACH might work in a hybrid fashion with the real-time PIN-debit networks, as FIS is demonstrating with PayNet. Such an accommodation might buy enough time to do a long-term rebuild of the ACH on a more economic basis than would otherwise be required (and provide a needed stimulus to the EFT networks and all of the smaller banks which are members of those networks). As well, an upgrade of notification messaging is likely to be an additional required capability in either build-out option; but this might be accommodated by working with the emerging digital/mobile front-ends using their inherent communicating modes (e.g., premium SMS, verified emails, etc.) to enhance the authorization messaging capabilities of the networks.

But the Fed should take a long and hard look at the costs and benefits of creating a new, purpose-built digital network with some of the design properties embodied in the ISO 20022 standard—i.e., adherence to a generalized, consistent framework with synonymous accommodations of data needs of specific users.

d. Enhancing the debit card network to enable ubiquitous near-real-time payments

Signature-debit cards mostly ride the credit card rails today; some 35% of Visa's sig-debit card transactions still take 2-3 days to clear and settle, and are just as fraud-prone as credit card transactions, so they are not good candidates for building a near-real-time payment option around. As well, just about all issuers lose money on sig-debet transactions under today's Durbin rates. On the other hand, PIN-debit is certainly a candidate for digital network capabilities, provided that something is done about the lack of merchant acceptance (only 35%) in the physical point of sale, and some consolidation in the presence and

policies of the more than dozen disparate PIN-debit networks is possible.

Further, an estimated 30% of FIs cannot today process a real-time authorization (due to antiquated and/or inadequate PIN-debit processing capabilities); to achieve the desired ubiquity, solutions for bringing such banking anomalies and participants into the digital realm would have to fashioned—or, failing that, a policy decision made relegating them to a separate, lower tier of product provision (if they are not able to achieve these upgrades with their higher, Durbin-exempt interchange rates).

Again, some hybridization of the debit networks with ACH might be the best near-term approach (as demonstrated by FIS, where its NYCE EFT network is made available on a private-label basis to support flexible interconnectivity). Such an accommodation is rife with business issues, however—especially how to provide the capability as an industry network 'utility' while provided by a for-profit processor provider(s)? More likely, as we've seen in a number of European countries, near-real-time debit will be provided by a number of alternative debit network options, requiring virtual (and physical) interconnectivity among those networks (e.g., Girocard in Germany, EAPS for European ATMs and POS, etc.). That is, until and unless a purpose-built digital network arises.

e. Implementing an entirely new payment system with the features described in the second desired outcome above.

Short of creating and providing secure functional frameworks for virtual currency-types of value-transmitting 'pipes' (as described above), it is likely that tokenization solutions will proliferate parochially in the near term. Tokenized payments and/or digital IDs can be infinitely flexible, and accommodated by any network that can properly determine the authorization decision and the destination information for the payment. But today's tokenization 'solutions' tend to lack the physical realm's risk management capabilities in ensuring authorized and valid account credentials and verification are used to set up services that provide tokens. Stolen account credentials can result in fraudulent tokens being generated and used downstream.

Moreover, tokenization schemes are proliferating without any discernible standards for security or compatibility (the TCH's Secure Cloud initiative, and the Visa/MasterCard/Amex 'copycat' alternative perhaps notwithstanding). It is simply not practical or economically viable for payment system participants to have to accommodate a multitude of different tokenization schemes with varying levels of security and related business terms and functionality (e.g., liabilities for transactions, capabilities and costs to de-tokenize to recover transaction information necessary for exception handling, etc.).

There are also other models for payments that should be explored and evaluated, such as the 'credit-push' alternatives in Europe (and NACHA's SecureVault product); electronic invoicing, post-purchase schemes (e.g., Sweden's Klarna and Dwolla/ADS's instant credit facilities); hybrid credit-debit cards (e.g., TSYS and various countries); merchant installment and financed spot-credit at purchasing (e.g., Brazil and other Latin American countries); various real-time debit systems (e.g., Dwolla, FIS PayNet, German networks);

and real-time access to linked funding accounts (e.g., 'sweep' accounts in the U.K.).

There are too many options cited above to explain each in the next four questions, but the essence of the examinations of them should be to get to the nature of innovations like American Express's Serve and Bluebird service offerings—as a fully virtual, interchangeable payment platform that can interconnect with any digitally-accessed network facility. Bluebird, in particular, is highly disruptive, but highly value-creating—both as a retail banking and merchant-provided alternative—if it can morph to independent, shared availability. As well, this investigation should examine the potential for obtaining a software-based, mathematical cryptography solution that could become an industry utility as the payment 'pipe' of the future.

i. What would be the most effective way for the U.S. payment system to deliver ubiquitous near-real-time payments, including options that are not listed above?

ii. What are the likely pros and cons or costs and benefits of each option? What rule or regulation changes are needed to implement faster payments within existing payment processing channels?

iii. Is it sufficient for a solution to be limited to near-real-time authorization and confirmation that good funds are on their way, or must end-user funds availability and/or interbank settlement take place in near-real-time as well?

iv. Which payment scenarios are most and least suitable for near-real-time payments? (B2B, P2P, P2B, POS, etc.)

Q7. Some industry participants have said that efforts to make check payments easier to use, such as by enabling fully electronic payment orders an/or by speeding up electronic check return information, will incrementally benefit the payment system. Other argue the resources needed to implement these efforts will delay a shift to near-real-time payments, which will ultimately be more beneficial to the payment system. Which of these perspectives do you agree with, and why?

Adapting today's payment system to accommodate significant volumes of paper checks in the future is at cross-purposes with both the need to harbor scarce resources for investments in the future *and* the benefit of weaning the user population—including and especially small businesses—from further using paper payments. As noted previously, the first generation of electronic payment alternatives have not been very successful at delivering a preponderance of user value:

- Electronically-processed checks (e.g., imaging) moves transaction information quickly and well, but inconsistency and apparent arbitrariness among banks in deciding how fast to recognize the funds availability confounds the utility and user experience

- Auto-debit and auto-pay makes it too hard to time or change electronic bill payments in the wake of erratic, unpredictable incomes, and results in excessive user overdraft fees, late fees and disconnects on use (some of which are less onerous when paying with paper checks)
- Account-to-account transfers among banks are still a mish-mash of varying timing, delivery capabilities and costs, forcing users to try alternative paths and services to gain capabilities
- P2P systems work well in limited-participation networks, but only interconnect via PayPal (or not at all).

All of these anomalies and deficiencies (and more…) tend to push users back to relying upon checks, while "the check's in the mail" conventions gain more usability in managing payments and finances.

The real solution lies in adapting electronic payments systems to the reality that the majority of U.S. households are living paycheck-to-paycheck, need more flexibility, but are still risk-worthy—therefore necessitating that DDAs and other payment system frameworks and policies provide more nuancing in policies and capabilities in order to quit penalizing good transactors currently constrained by outdated (and one-sided) electronic payment offerings.

Q8. How will near-real-time payments affect fraud issues that exist with today's payment system, if at all?

i. Will near-real-time payments create new fraud risks? If yes, please elaborate on those risks.

Near-real-time payments can eliminate most funding risks, but the pace at which funding commitments travel is likely to be a good deal faster than today's compensatory controls and risk checking systems can accommodate. (This unfortunate condition has been largely influenced by the deficiencies of the signature-debit card product, which purports to be a 'debit' card transaction, but is much more like a credit card payment in terms of behavior, risks, and costs to the system.) And the ACH was never designed for real-time. These risk management systems will therefore need to be upgraded to avoid transaction risks of funding commitments being compromised too quickly for controls to prevent them.

The key is to figure out how to implement sufficient controls on the *settlement* processes to avoid serious transgressions. As most payment settlements will remain dominated by regulated bank accounts (at least for a decade or more, if not for a lifetime), the banking industry must be able to build and monitor settlement system operations to account for real-time risks (both of fraud and error). One solution that has been advanced is 'virtual' settlement, wherein companies (such as merchants) can reconcile funds delivery for 'safe' transactions, while holding accounts suspend money movements until adequate verification measures are deployed. Another part of the solution is to tier transaction risks according to specific features (especially timing and size of delivery of funds) and on the basis of risk; similarly, users could be assessed tiered fees for pushing delivery (e.g., in an expedited payment need scenario) that might override system controls.

Adapting this 'back-end infrastructure' to digital payments is another essential element of the transaction experience overall, and a new payments paradigm would necessarily have to provide for it in a consistent and sustainable way—probably shared among providers to ensure consistent and predictable user experiences. There are a small number of startups that propose to do this very thing—focusing on mobile payments for now, but the costs of building and supporting an industry entity and utility will be sizable for anyone—and therefore likely to be the province of banks. If not funded by payment fees, then such system enhancements would need to come from related new revenue models, such as commissions from marketing offers and programs, or wholly new business models—such as providing digital IDs—that banks could logically transition to as an augmentation or replacement their roles with payments.

Q9. To what extent would a ubiquitous near-real-time system bring about pivotal change to mobile payments?

Aside from the minimally used mobile payments variations that utilize stored credit cards, and the still small, but growing use of debit and prepaid accounts for some limited-participation network offerings (e.g., Serve), the most prolific mobile payments deployment yet is Starbucks' two-dimensional bar code token. Users load and present this token from their handsets for scanning at POS counters. While they are waiting in line, most users of Starbucks prepaid store card check their account balances and, when desired, reload their accounts (often via PayPal) or decide to redeem loyalty rewards. Starbucks' card accounts generate more than 30% of its volume, and 2/3 of those cardholders are now using this mobile payments application. Even at Starbucks, which is an investor in Square, the use of Square's mobile system for credit and debit card payments is quite modest. So, from the buyer's perspective, there is little so far about the proposed new payment paradigm that moves the needle forward on choosing to pay via mobile—outside of limited-participation networks that need special account set-ups.

From the seller's perspective, there has also been little tangible interest in moving to new payment paradigms—outside of the frequent use of prepaid store cards by QSRs (e.g., Burger King, Dunkin Donuts, Subway, etc.) in order to process lower-cost transactions where they can. We have seen this payment-cost-reduction reality surface with contactless and NFC payments as well, where merchants have been very conservative about offering mobile payments capabilities—even when the material costs of changing out in-store check-out and payment terminals is subsidized—because of the potential for converting low-cost cash transactions to standard credit cards, *and* debit cards, which—even at lower post-Durbin rates overall, cost low-ticket QSRs and coffee shop companies 50-100% more in interchange than they were paying before Durbin. (The card brands treated the $.21 Durbin-intended 'ceiling' as a 'floor' for rates.)

NFC, because it emulates cards and perpetuates existing payment behaviors, rates and rules, has experienced very little merchant traction. Instead, many merchants have either signed on to the Merchant Customer Exchange consortium (MCX, the merchant-owned mobile wallet initiative), which

now has the support of several dozen of the nation's largest retailers, or have not committed to a mobile solution yet in the hopes that a more balanced and cost-effective array of payment options emerges. Ubiquitous, near-real-time payment options—if they reduce costs and expedite payment consummation at much lower levels of risk, fraud and exceptions—would certainly seem to address this need from the seller side.

In addition, many new online (e.g., Groupon, Yelp, OnTable, Braintree) and offline (LevelUp, PayPal, Amazon) business models are emerging where the payment function is embedded, and transparent, in applications that drive the user experience primarily through innovative marketing functions. If ubiquitous, near-real-time payments become a means of facilitating this new interactive, digital commerce paradigm—where the payment 'gets out of the way of' better buyer-seller interactions, and is priced fairly, in proportion to its new value as a 'facilitator' (but not a driver) of mobile technology use, greater traction can be expected from this factor as well.

That said, consumer value—other than today's unfiltered barrage of coupons, discounts, loyalty programs and other marketing promotions and programs—remains elusive. It is too early to tell how much embedded, transparent payment presentation will impact consumer adoption (except for venues, such as bars and restaurants, where many consumers are reluctant to hand over their plastic payment cards given the skimming problems). So for mobile payments to 'take off,' the key aspect right now is getting merchants to drive usage.

MCX plans to do that with some new types of debit and credit payment forms riding on the FIS/NYCE private label network rails. One rumored type is a decoupled debit card variation, which MCX had intended to produce a $.04 payment cost. But if 'Durbin 2.0' (Judge Leon's intervention) is sustained, it is possible that debit card fees will drop to $.07 or lower—obviating much of the need for that merchant-provided variation. Under such circumstances (and assuming MCX moves into a sustaining position in the mobile payments marketplace), banks will have little choice but to move to a near-real-time payments capability in order to make any money on their debit card accounts.

Q10. What would be the implication if the industry and/or the Federal Reserve Banks do not take any action to implement faster payments?

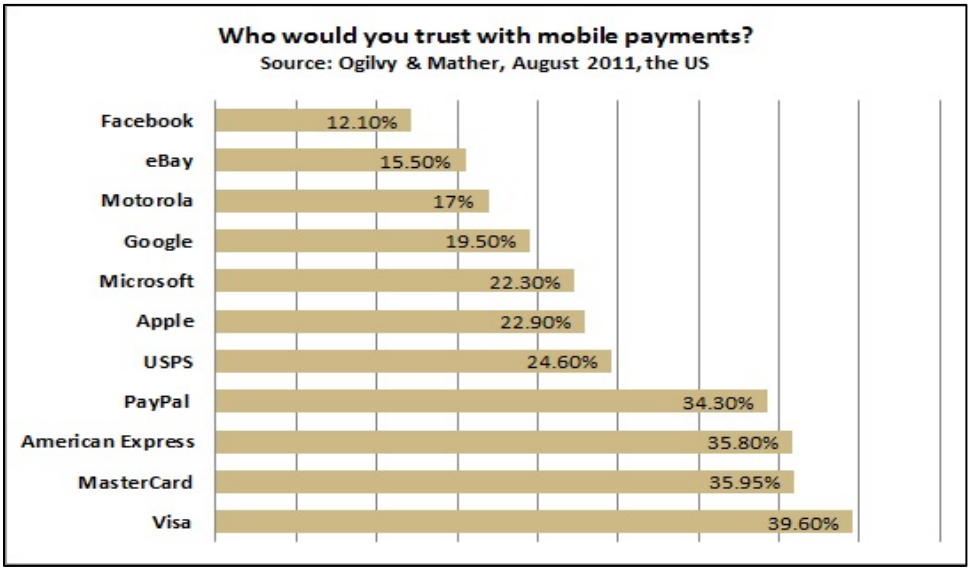
i. What is the cost, including the opportunity cost, of not implementing faster payments in the United States?

To a significant extent, while acknowledging that the notion of a government body 'picking winners and losers' in the marketplace is another third rail of politics, banking *is* an exception. Assuming that there is consensus at a national level that a viable financial services industry is essential, and assuming that a large majority of digital transactions will continue to be funded from regulated financial institution accounts, then banks *have to* participate in digital payments in one way or another. Participation the way they have with signature-based card payments seems highly unlikely, given the growing resistance to the

vestiges of that participation from merchants and regulators (and some in Congress). So what form will continued participation in payments by banks take?

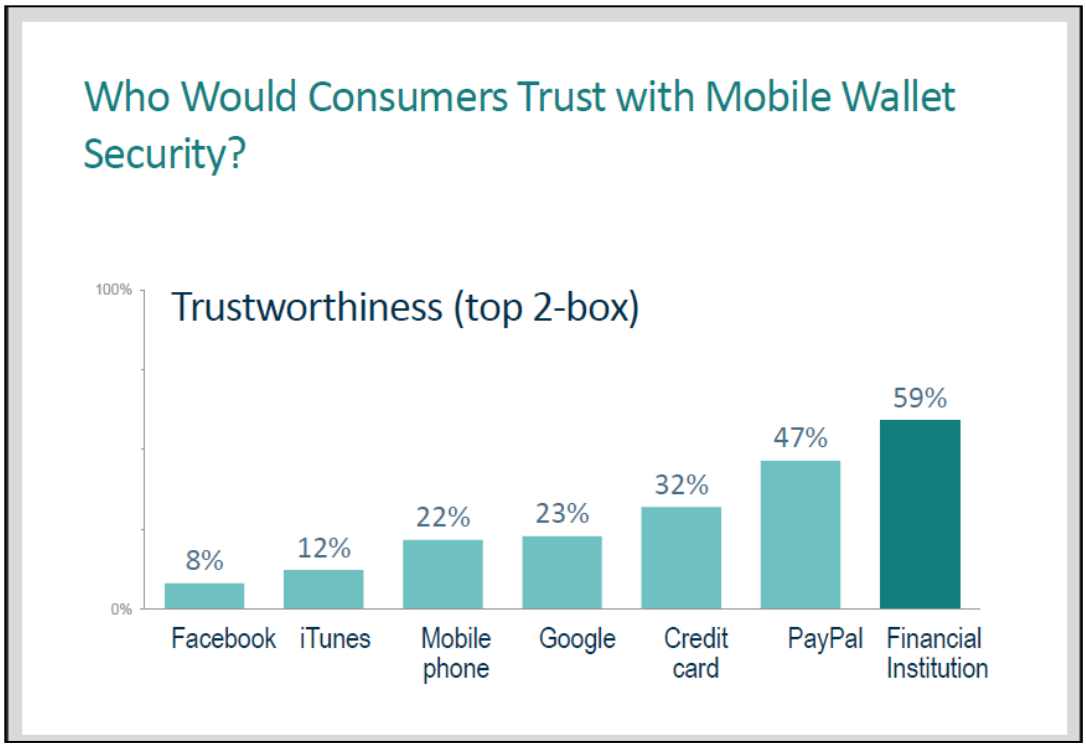
Adding real value—which faster payments would certainly do—is a big plus, as noted previously. Pricing that value at cost-plus-reasonable-return would be another big plus. Participating constructively and openly in a Fed-convened body that represents the entire payments ecosystem is another major contribution. But perhaps the largest upside for regulated financial institutions in the transformation to faster payments is the ability for FIs to leverage the inherent trust consumers and small businesses have in them—before digital companies either a) ruin the party for everyone by violating consumer privacy/exposing data; or b) replace banks by becoming the only viable, default provider of digital payments.

This proposition can be illustrated quite well by looking at two research findings that occurred about the same time nearly two years ago. The first one is typical of most surveys asking who consumers trust with mobile payments:



Note that the card brands, along with PayPal, rate highest—vis-à-vis other providers—especially the big digital companies.

But research often has to be viewed in the context of who paid for it and what were they looking to find; so a separate, but parallel survey found that when the reference to people's primary *bank* is included among the choices, *that* option becomes the top choice:



Source: Market Strategies/First Data

The trouble is, when consumers are asked which providers they trust most with their personal, account and purchasing data, the opposite order results—digital providers are far more trusted with knowing how to protect this information and keep it under the consumer's control. This translates to a *huge* exposure for FIs, as the drivers for commerce shift from payments to marketing information and—eventually—digital IDs.

Faster payments, then, becomes the 'qualifying' factor for banks to participate gainfully in electronic commerce. The 'differentiating' factors will include how banks participate marketing value propositions, and whether—instead of, say, a Google+, or Apple iTunes, or Facebook log-in ID, the buyer/payer uses the digital ID provided by regulated financial institutions.

Q11. To what extent will the industry need to modernize core processing and other backend systems to support near-real-time payments?

i. What is the likely timeframe for any such modernization?

As mentioned previously, there are many limitations on providing faster payments (and digital transacting) extant in the existing FI infrastructure. We know, for example, from recent experience that the banking industry has great difficulty upgrading core services such as DDA systems at the upper end of the market. Smaller FIs struggle financially across-the-board with payments—e.g., they provide debit card payments at an average cost of $.75! In-between, few FIs have the investment resources available (in part due to spawning requirements for regulatory compliance) to upgrade their core processing and other back-end systems to move to digital directly. Thus, any systematic

upgrading of individual bank systems to 'go digital' is likely to be an extended, expensive and hard-to-justify experience overall.

As a result of this proposedtransition to faster payments, most FIs will be confined to providing core account authorization and funding capabilities, along with adjunct facilities for account holds and suspension of funds to support good funds product models. The normal tendency for the industry would be to require even more dependence on either existing third parties (i.e., FIS, Fiserv, Jack Henry across an array of integrated services, and many dozens of other providers such as IBM, NCR, Diebold, etc. for specific products and services), or from new, adjunct providers for digital services (e.g., PayPal, Monitise, even Visa and MasterCard). This support could transpire quickly—say within 3-5 years.

Thanks to the work of NSTIC (the National Strategy for Trusted IDs in Cyberspace), the Open Foundation, and other government and industry collaborative efforts, there is now a considerable and growing foundation for making digital identification, authentication and verification a reality. This 'movement' will take 5-10, but it represents the best business model going forward for regulated FIs. But they will not get there if they do not participate in providing faster payments in the first place; it's the price of admission for being a part of the payments of the future.

Q12. Some industry participants suggest that a new, centralized directory containing account numbers and routing information for businesses and/or consumers, to which every bank and other service providers are linked, will enable more electronic payments. A sender using this directory would not need to know the account or routing information of the receiver.

i. What are the merits and drawbacks of this suggestion?

Reaching the 'nirvana' state of faster, digital payments will require that members of the payments ecosystem trust and rely upon a funding 'pipe' wrapped in common infrastructure functions (and choices) that ensures the security, usability, and reliability. Tokenized payment 'cryptograms' that are authenticated in the cloud, with authorizations pass to the merchant or biller, and settled appropriately to the type of transaction are the key components of this build-out. But such a build-out will logically require either a) interoperability and compatibility among many diverse system, or b) a 'master' directory from which all relevant pieces of data in and around the 'pipe' are assembled in-concert and made available to qualifying participants of the emerging ecosystem.

In the first instance, the marketplace will need to define the mechanisms to interoperate and the standards (e.g., industry APIs) to ensure compatibility, and have to develop a cryptographic key structure that supports many, linked families of provider user bases. This could best be done by recognizing and accepting digital IDs, rather than exposing actual account identifiers. Routing information can still be provided by BIN-like numerical structures in order to ease processing efforts. In a sense, this 'connectivity structure' would come together like an array of ISO 8583 variations used today in the card payment industry to accommodate a wide set of variations built upon a common parlance and structure for the minimum necessary data needed to complete a payment.

In the second instance, a high degree of centralization is implied, which could present a new form of systemic risk if ever compromised. To avert such a threat, the physical consolidation of data (e.g., accounts linked to a specific individual or business entity) can (and will) be provided for regulatory compliance. But all other aspects of centralization, including and especially the cryptographic key hierarchy can (and should) still be decentralized—albeit with a common root key if it can be protected. So there is some flexibility possible in such a design. This option 'feels' more like the ISO 20022 standard's design, with the payment information and functions embedded in consistent way (like a math/crypto pipe), and the spawning information needs accommodated in specific families of content requirements. And it would be considerably easier to develop this type of directory in a cloud structure supported by a new, purpose-built digital network.

ii. What is the feasibility of this suggestion?

Many younger consumers appear quite willing to expose highly personal information about themselves to marketers looking and willing to pay for more intimate contacts with them. Many payments system veterans (and consumer advocates) worry that once this information gets loose, any hopes for privacy and data security go out the window. The solution, of course, is transacting with digital ID—one that can accommodate a variety of user 'opt-in' choices of privacy settings and permissible use of data. Yet the notion of a 'national' ID elicits apoplectic reactions from some.

The White House's NSTIC initiative takes cognizance of this changing distinction for what happens in cyberspace, where effective identification processes can dramatically improve not only security and privacy, but greatly enhance convenience and extend access to products, services, information and content provision that are becoming such a dominating part of our digital existence. It is hard to see this happening without extensive involvement of banks, though it is equally difficult to ascertain any meaningful bank involvement in NSTIC or other prominent government initiatives (smart card projects notwithstanding) to this point. And without Fed intervention, it is also impossible to imagine equitable, judicious and holistic bank inputs be contributed.

Electronification

Q13. Some industry participants say that check use is an enduring part of the U.S. payments system and that moving way from checks more aggressively would be too disruptive for certain end users.

i. Is accelerated migration from checks to electronic payment methods a high-priority desired outcome for the U.S. payment system? (Accelerated means faster than the current trend of gradual migration.)
ii. Please explain, if desired.
iii. If yes, should the Federal Reserve Banks establish a target for the percent of noncash payments to be initiated via electronic means, by a specific

date? For example: "but the year 2018, 95% of all noncash payments will be made via electronic means."

iv. What is the appropriate target level and date?

The most sensible (but politically charged) approach is to charge users for the costs of their paper checks. Otherwise, the U.S. faces the specter that the 'last check in the system' will cost billions of dollars for processing assets that have to remain in operation to accommodate non-electronic usage. There can be a transition period, of course—particularly for elderly users; but new 'checking' accounts should be classified and assessed fees directly for 'checking' options and services, and those costs should no longer be subsidized either by banks or check accepters. And a review of electronic bill payment practices—especially the difficulties with and punitive fees associated with user needs to get more flexibility in the timing of those payments—should be reviewed (please see next question). The Fed could and should lead industry initiatives that pursue this new course; electronification rates will follow accordingly.

Q14. Business-to-business payments have remained largely paper-based due to difficulties with handling remittance information. Consumer bill payments also are heavily paper-based due to the lack of comfort some consumers have with electronic alternatives. In addition, many small businesses have not adopted ACH for recurring payments due to technical challenges and/or cost constraints. The payment industry has multiple efforts underway to address these issues.

i. To what extent are these efforts resulting in migration from checks to other payment types?

ii. What other barriers need to be addressed to accelerate migration of these payments?

iii. What other tactics, including incentives, will effectively persuade businesses and consumers to migrate to electronic payments?

iv. Which industry bodies should be responsible for developing and/or implementing these tactics?

B2B and small business payment needs have been unrequited for decades, so their continued dependence on paper checks for the majority of their payments in not a shocker. A good example of this continuing problem is the poor reputation for usability incurred by the industry's most popular small business accounting programs—despite more than two decades of experience with 30 million users. The source of this problem is arcane accounting conventions married up to parochial IT requirements; electronic payments struggle to make this unhappy marriage function better, but even aspirational solutions (such as NACHA's ebids initiative for e-invoicing and small business payment portals such as PaySimple) struggle for adoption.

Big companies seem to insist on doing things their own way, but the building momentum for ISO 20022 offers the prospect for unifying the way things are done business sector-by-business sector—while still standardizing the underlying movement of the funds. Small businesses will seemingly only be accommodated once the Googles of the world figure out how to streamline their

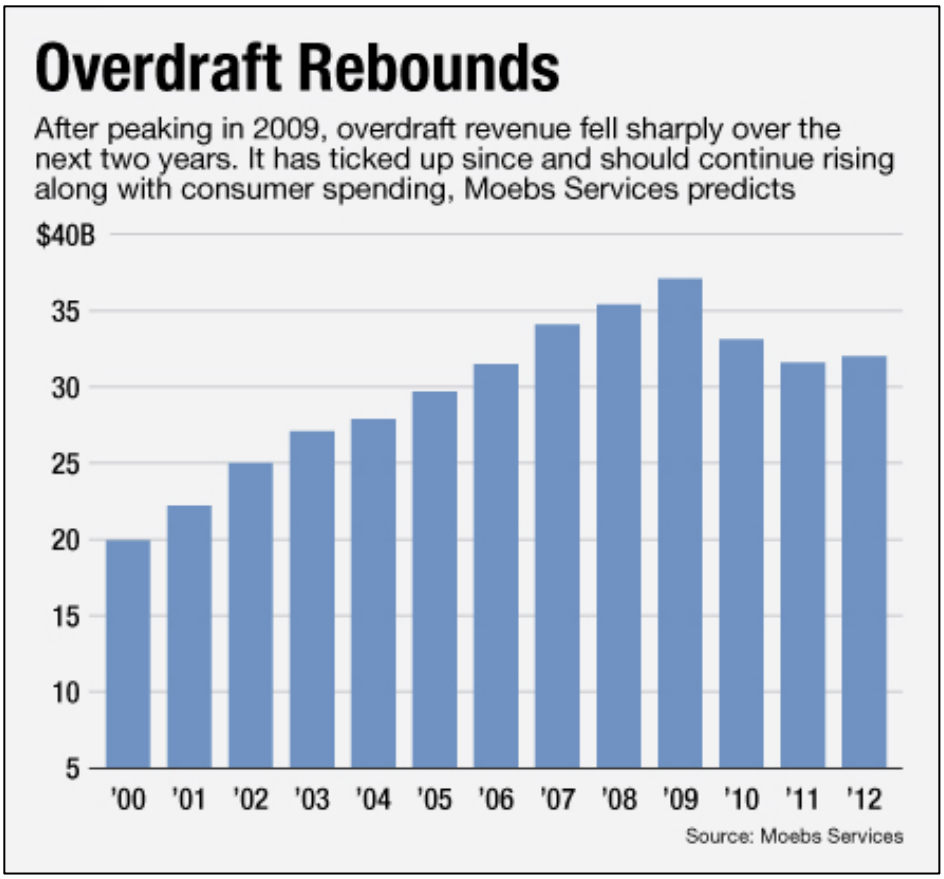
digital lives—most likely giving them a compelling financial incentive in order to unshackle them from the constraints of today's IT/Accounting software regime. (surrendering valuable data about themselves in the process).

Electronic bill payment is a great example of this disconnect in today's electronic payment options. Signing up for automatic debits and payments is nominally a good indication of a consumer's (or small business's) intentions to pay (and therefore the level of risk they pose). Once properly set up, 'auto-debit' or 'auto-pay' options can ensure timely execution of payment (albeit 20-25% of bank consolidator bill payments ultimately still wind up as checks because of inability to move funds to mostly smaller billers electronically…). But under cash-strapped circumstances, such as erratic flows of income in these uncertain economic times from multiple jobs (or lines of business), automatic payments often prove expensive and counter-productive.

If a consumer (or small business) doesn't have adequate funds in-place at the time of the automatic debit or payment, the electronic payment execution occurs anyway, typically resulting in an overdraft (or over the credit line) fee from the payment account (and, if not actually paid by the account-holder to the biller) possible late-fees as well. With checks, the payment delivery can be timed—making some assumptions about delivery modes and posting requirements—and many of these fees can be avoided as a result. But even use of checks, which gave consumers (and small businesses) the perception of control (and billers and merchants the perception that the payments were made…) is difficult to time these days, as banks have radically different policies and timeframes for clearing checks, recognizing deposit funds, scheduling due dates, and managing the staging of debits and deposits/payments within given accounts.

There are similar problems at the biller end. Stories abound in the industry about the difficulty in getting billers to update which cards or DDA accounts the consumer (or small business) wants to use; the biller often 'hits' the original payment account (sometimes repeatedly) rather than making the change expeditiously. This can result in multiple $30-35 overdraft fees for the user, who was anticipating payment from a different account, and who didn't have the staging funds for payment in existing or closed accounts. And in this regard, small businesses share their digital 'needs' with consumers. Cashflow is still king, and much of the industry's solution for electronic automatic *penalizes* users, rather than empowering them.

The end result is that, according to recent research, and despite legislation a few years ago aimed at reducing these types of problems, overdraft fees on DDAs are rising again, and remain more than $30 billion a year:



The banking 'system', then, is apparently failing to make electronic payments cost-effective for many users. So why would we be surprised to see adoption of online bill payment stagnating, as it has in recent years?

That said, the bigger intrinsic problem in 'banking' is that most of the transactional systems assume that the user (consumers and small businesses) *always* have necessary and sufficient funds predictably on-hand whenever payments are due or made, and imposes substantial penalties on users when that funding is *not* immediately on-hand—even though the user had demonstrated (and tried every way possible, in many instances, to effect) the intention to pay.

This more fundamental complication, in a period of wealth deterioration for much of the middle class (along with the alienation of more than 20% of the population from banking products altogether—the unbanked), requires a fundamental re-thinking of the role of banking—both in helping customers manage their finances and enabling ubiquitous financial product access (such as lending). In persisting times of erratic incomes and account funding, rigid, arbitrary, inconsistent and penalty-prone payment and account management policies and conventions drive users back to paper. Until this systemic problem is addressed, full adoption and use of faster electronic payments cannot be assured.

Cross-border payments

Q15. To what extent would the broader adoption of the XML-based ISO 20022 payment message standards in the Unites States facilitate electronification of business payments and/or cross-border payments?

The corporate B2B sector of the economy needs and deserves the benefits of electronification, and we hope it is received in the expected 5-10 year timeframe with adoption of ISO 20022. It is expected that the Fed's plan to derive a business case for adoption this standard will prove to be compelling. The question remains, though: what about small business (and even consumer) use of cross-border payments?

If you do a bank wire transfer, the end-to-end fees can be $40 or more. Western Union remittances, depending on the destination country, can cost $10-$40 for just $300 transmitted. Credit card companies charge 3% for "currency exchange" fees. PayPal often charges the standard rate of 2.9% plus $.30. Will these users have cross-border solutions that they can take advantage of? Is there a SaaS (software as a service) configuration option for ISO 20022? If, as a national goal, the U.S. government (including the Fed) wants to encourage global commerce, then a digital payments 'platform' will need to include cross-border services and capabilities for users other than large corporations.

Q16. What strategies and tactics do you think will help move the industry toward desired outcome four—consumers and business have greater choice in making convenient, cost-effective, and timely cross-border payments?

There are lots of other complicating factors in cross-border commerce besides payments—i.e., customs declarations and processing, tax consequences and obligations, shipping, delivery and fulfillment requirements and options, exception handling processes and capabilities, and payment consummation complexities. These complexities are likely to grow even bigger as payment options expand (along with differences in funding timing, guarantees, service levels, costs, etc.). Providing the necessary educational support is difficult to cost-justify for low-volume users, though everyone would still like to encourage their cross-border commerce.

So one thought might be to design a global commerce resource infrastructure (perhaps built in concert with the post office facilities and websites?) that arrays supporting products, services, and educational information (and perhaps even training?) around payment and payment related functions and options. In theory, this infrastructure could be provided by banks (and even help leverage bank branch operations, which need more usage and revenue to keep open in many areas). But in this arena, payment options *will be* the main driver of the value proposition by making global commerce both affordable and efficient.

Safety

Q17. Payment security encompasses a broad range of issues including authentication of the parties involved in the transaction, the security of payment databases, the security of software and devices used by end users to access payment systems, and security of the infrastructure carrying payment messages.

i. Among the issues listed above, or others, what are the key threats to payment system security today and in the future?
ii. Which of these threats are not adequately being addressed?
iii. What operational or technology changes could be implemented to further mitigate cyber threats?

Humans remain the biggest points of vulnerability for security, and the weakest links for deployment of sound security practices. Yet the card-based payments system tends to absolve cardholders of most if not all responsibilities for protecting their account credentials and devices (e.g., 'zero liabilities for fraud', which encourages both unsafe device management and use of credentials, and covers up 'friendly fraud'—where the cardholder denies the transaction falsely; the latter is reported to be 30-40% of fraud and chargebacks experienced by some online merchants). Remote commerce—i.e., phone order, mail order, online and now—so far—mobile transacting—forces merchants to absorb all the liabilities for charge-backs and disputed transactions, shoulder most of the costs for risk mitigation, and pay premium fees for so-called "card not present" (CNP) payments. Such an off-loading of fraud mitigation responsibilities makes little or no sense in today's environment (and even less so applied to mobile transacting).

As well, there is the problem of charge-back 'recidivists': at MasterCard in the late 1990s, a few hundred thousand cardholders accounted for 2/3 of total chargebacks; when issuers finally grew weary of dealing with the customer services problems, they simply bounced to another new issuer. For the ACH system, it has only been in the past few years that a 'bad actor' list of problem originators has been seriously considered. So there is little accountability in today's payment system for human risks. Yet the current view is simply to port the practices on these existing networks forward into the wild frontier of systemic open network attacks and threats. That movement would seem to be terribly ill-advised under the circumstances.

Such an industry quandary raises the question of whether a new, purpose-built digital network would better serve American society than perpetuating one-sided existing networks. But when you consider the most likely alternative—i.e., upgrading the ACH network to serve much broader purposes and uses—creation of a new network from scratch would seem to have a number of advantages. For example, the ACH network relies to a significant extent on borrowed or shared computer facilities; it will need to need upgrade to linked, peering data centers operating independently and fortified with the best network intrusion capabilities. Similar improvements will likely be needed for bank *internal* systems as well. And connections to other open networks and limited-participation networks will need to adhere to standards developed for both existing and new digital networks if they use or transport bank-regulated accounts. On top of all these considerations, there is the problem of ACH formats—now two generations old and extremely difficult to work with; these would have undergo an ISO 20022-scale of redesign to meet emerging digital requirements. All of this will be

expensive, and require extensive collaboration among most of the participants in the payments ecosystem.

One recommendation to the Fed, therefore, is to commission a working council (of industry experts from providers and consulting firms) to weigh the requirements of a fully digital, ubiquitous, near-real-time national (and global) network, with detailed cost-benefit analyses of the purpose-built versus the digital conversion of existing network options (such as the EFT networks, and/or the ACH). This investigation should also factor in associated costs to society (e.g., merchant interchange fees, consumer overdraft and credit usage fees, issuer charge-offs, and the *total, real* costs of fraud for the entire payments ecosystem) in order to legitimately address a full measure the costs of continuing to do nothing (other than tweaking today's inefficient and fraud-prone systems).

Q18. What type of information on threat awareness and incident response activities would be useful for the industry?

i. How should this information be made available?

We understand that the Fed has received internal proposals a number of times over the past decade to create a superordinate structure residing above the payment brands and banks for the specific purposes of collecting and assessing data on risk management threats, deriving actual fraud data (and costs) for the entire industry (including for merchants), and evaluating threat mitigation technology and practices for sharing across the industry. Each time, concerns that bigger banks which have invested heavily in risk mitigation for both self-protection and as a source of competitive advantage (particularly for business customers) would in effect 'subsidize' the rest of the industry, coupled with concern that the Fed would use actual fraud data to promulgate additional regulations (including fee restrictions and/or assessments), have dissuaded the Fed from proceeding with such an initiative.

Unfortunately, this 'laissez faire' approach has resulted in very high rates of fraud produced in the global payment system by the U.S. (half of all fraud on one-quarter of global payment card transaction volume, for example). As well, merchant fraud, which is rarely counted accurately, has been estimated to be $40-$100 billion—many times the costs experienced by banks and networks. The black markets for stolen credit card credentials (as little as $.15 for a full set) and DDA numbers and access (sold for as little as $2 each) are flourishing (and doing embarrassing things like funding Al Queda field operations via website links). PCI costs for merchants between 2004 and 2010 were an estimated $20 billion, according to a survey by the Merchant Advisory Group, while total card fraud (for banks) amounted to just $13 billion during that period. It is no wonder, then, that there is a growing perception that the U.S. has become a 'backwater' of payments efficacy.

It makes little sense, then, for 14,000 banks and credit unions to tool up individually to fight fraud (especially in the futile effort to perpetuate magnetic-stripe/plastic card practices, such as exposing payment card credentials in the clear, in operation as long as possible). It makes even less sense for the

industry to invest another estimated $8.6 billion in moving to chip-based smart cards via EMV/NFC, when the payment brands and big banks are promoting risk-prone card-emulation option (which also perpetuates PCI compliance costs by putting card account credentials into the clear at merchant terminals). A Fed-convened roadmap for defining and sharing best practices for security, and pushing the industry to do better than card-emulation mode options for chip, seems more appropriate (and urgent) with each passing day.

Finally, the more the industry learns from data breach incursions and how to minimize the damages (short of accelerated eradication of the mag-stripe paradigm, the better; this will also require more sharing among industry participants—something that appears to be impossible to achieve without an institution such as Fed, in concert with appropriate industry groups, "leading" the way (and while protecting the use of the fraud and cost data, including by its regulatory arms…).

Q19. What future payment standards would materially improve payment security?

i. What are the obstacles to the adoption of security-related payment standards?

Improving the efficacy of EMV and NFC would be a great start (as discussed in Appendix A). Both programs, as mentioned previously, are facing mounting opposition from the rest of the payments ecosystem; neither new payment mode appears to have a compelling business case for deployment—even by banks. Rather than simply leaving these standards to EMVCo (owned and controlled by the card brands), the Fed has convened a working group (in early December) to discuss whether the entire payment ecosystem—and society in general—would benefit from creating improved standards through a broader and (ostensibly) more objective standards group like X.9.

For the longer term, a more proactive, future-oriented approach is called for. For example, the EMV protocol specification development began in the mid-1990s, and was driven by business conditions (i.e., the high cost and unavailability of doing real-time authorizations in many countries outside of the U.S.) that no longer drive business cases. With most of the world moving to digital transacting over the Internet and wireless carrier networks, a new standard for digital interactions on mobile devices is clearly called for. Moreover, EMV was never designed to accommodate merchant access to a choice of debit networks—so it is currently non-compliant with the Durbin Amendment mandate—a development that is creating further rifts among industry participants and further delays in shedding the fraud-prone mag-stripe paradigm in the U.S.

The simple explanation to problems like these is just competing business interests and objectives of the participants, which the marketplace can resolve. But in the U.S., there is little along the lines of meaningful competition by payment providers. Legacy system participants make a lot of money out of payments ($300 billion a year, according to McKinsey & Co.), and prefer to leave things just the way they are. Fraud costs represent a *tiny* portion of revenues banks make (e.g., merchant interchange, overdraft fees, etc.) or total costs they

incur (e.g., huge charge-offs on signature-card use, legal fees lawsuit settlements, regulatory judgments, etc.). So why change things until banks and brands absolutely have to?

But society is increasingly not well-served by the legacy payment system, and the longer constructive changes are fended off and delayed, the more embarrassing this system is to this country. When Al Qaeda websites advertise where to get stolen credit card credentials from thriving black markets in order to build IEDs, it is impossible to justify the status quo. This industry will not fix itself. And it should no longer tolerate trading off security and privacy for legacy profit margins.

Q20. What collaborative actions should the Federal Reserve Banks take with the industry to promote the security of the payment system from end to end?

The Fed needs to get off the sidelines, and become a proactive participant in shaping the payment system for the next century (we're already 13 years behind…). It should convene the key participants, get them commit to achieving consensus, monitor and referee (when needed) disputes, and prod and nudge the ecosystem into developing sound and efficient solutions worthy of the democratic heritage of this nation.

The Fed needs to operate *above* the brands and the banks and the rest of the payments ecosystem, working with other regulators to provide appropriate guidance and direction the way other similar bodies have done in Canada, the U.K. and many other advanced societies. It is imperative to begin with defining and building better standards for security, privacy and fraud mitigation. From there, the nation—and the industry—must move forward to embrace the full potential of digital payments to empower all of its citizens with the ability to transact in any venue and setting with full confidence that the safest, soundest and most efficient system possible is operating for their benefit.

Q21. Please share any additional perspectives on U.S. payment system improvements.

[Please see Appendix A: The Challenges of EMV/NFC Adoption in the U.S., which accompanies this response]