# Partial Response to
# Payment System Improvement - Public Consultation Paper

**Ed Oppenheimer**
**10/17/2013**

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

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

**Response**

**FED:** 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.*

Disagree somewhat: Non-institution check receivers cannot immediately convert the instrument into an accessible deposit in a FI. This is easily possible and because it is not available rewards institutions sending checks due to interest gained by the float. I believe if any check becomes an electronic check (E-Check), then there would be an incentive for institutions to originate payments by electronic methods especially a small value gross real time payment system (hereafter referred to as SVRTP). I believe incentives for institutions sending checks (if SVRTP available) diminish because then it would be less expensive based on the following assumptions.

Given: check for $1000.00

Costs: FI pays mailing and overhead costs = $0

Income: .8 % PA = (1000*.008)/365*(days of float) = c. $.02 multiplied by days of float.

Given: ACH for $1000.00

Costs: $25/month plus .10/ check

Income: $0.00 (1 day float possible)

I believe if a SVRTP would be available then the costs for use based on small values and heavy traffic will be lower than ACH (and less risky than ACH due to quicker time for settlement). The cost per check may increase, as FI require more fees to use the buggy whips and the income would reduce because of the reduction in float time. Once the costs for checks increase to the point where they exceed income then check use will diminish exponentially.

**FED**: 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. 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.*

I disagree that US payment systems do not have the capability to clear transactions in real time (debit card transactions particularly). Here and in Europe (EMV based solutions) debit transactions require a PIN and so real time authorizations occur in microseconds[1]. Settlement in the US uses ACH. Britain for example uses FPS, which is also a deferred netting system, so I would say that two systems use the same methods for clearing and settlement, whereas periodicity of settlement is configurable and therefore not relevant to the discussion.

**FED**: 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).*

The term "Most recent payment innovations" is too vague; no comment.

**FED**: 4. *Some features that are desired increasingly by end users are generally lacking in many legacy payment systems, such as –*

*o 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;*

*o Assurance that a payment will not be returned or reversed;*

*o Timely notification to the payer and payee that the payment has been made;*

*o Near-real-time posting / availability of funds to both the payer's and payee's accounts; and*

*o 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*

I agree all features are good ones to have in retail and small value payment systems.

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

I agree and find it unacceptable.

---

[1] I am a traditionalist and do not use the term "near real time" and prefer to use the term "real time" and then in technical discussions describe the particular nature of logical holes in time based on the actual path a transaction takes.

**FED:** 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.*

*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.*

There is great potential for mobile devices, but security needs better engineering. The risk of data intercept with any wireless communication protocol remains the biggest obstacle to growth. Merchants that accept payment from a wireless device must pay the CNP surcharge, so, using a secure point of sale (POS) device, is less costly by a significant amount. EMV security protocols (using combined data authentication (CDA) and PKI) still can be penetrated by a lunch room attack. Fortunately, the "valuable information" used with security protocols effectively foils a lunch room attack in theory and therefore reduces the surcharge on phone initiated transactions.

**FED:** 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.*

As object oriented software becomes ubiquitous, larger firms will have the capability to maintain software at lower costs. Payment object replacement allows the payment industry to give black box "parts" to firms. The Fed can do something to speed the dinosaurs along the path of righteousness.

Tagged based protocols such as ISO 20022 (Payment vs demand protocol) must be the future for initiation of transactions that now are a hodgepodge of VISA (I, II) and roll-your-owns. Acquirers translate these diverse data sets to the archaic bit mapped ISO 8583. If the Fed convenes a technical group to first define all possible fields and their possible values, and then creates a tagged protocol for the initiation of payment from personal electronic devices, then firms can easily create payment objects from that specification and allow quick upgrades when needed.

Such a strategy gives firms an ability to evolve their defenses against evolving attacks. The dialectic between cops and robbers shows slow responses against constantly evolving attack. Well defined industry standards gives firms a rapid response option against thieves.

**FED:** 8. *Consumer fears about payment security sometimes inhibit adoption of electronic payments.*

More to the point, retailers facing surcharges from initiating transactions from personal electronic devices inhibit the adoption of electronic payments.

**GAPS**

One gap (and therefore an opportunity) the paper missed completely was the need for an international standard for payment message structures originating at a POS device. The opportunity exists to create such a standard based on ISO 20022 regardless of the final clearing or settlement path.

Another gap is the need for an international clearinghouse of Reg. E type claims. Fraud increases because there is no methodical way to track it and plot its trends. The opportunity to create a clearinghouse for Reg. E claims exists.

The biggest obstacle to a gross real-time payment system for small value payments is interchange fees. Banks guard this revenue with lobbyists and campaign contributions and the Federal Reserve's reticence to threaten those fees prevents a Fed's service offering of a SVRTP.

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

i. What other outcomes should be pursued?

**Response**

The Fed should offer a SVRTP. Anyone in the world should be able to log on to a secure web site and receive either a vendor number or a consumer number associated with an account that can receive or push payments. Buyers push payments into a vendor account after the validation that the buyer is the buyer and not an impostor.

Transactions originating from a point other than a vendor establishment do not originate as a payment request from an on-line vendor. Instead, a buyer originates a transaction from the Fed app that deposits the value immediately (24/7) into the vendor account. The vendor sees the result of the transaction, but has no other details. The Fed provides notification to both vendor and buyer. The vendor FI may delay posting the funds to the vendor account as determined by rules.

The Fed would continually need to advertise the service in many mediums until it is ubiquitous.

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

**Response**

The Fed should operate a SVRTP. The Fed should sponsor an international Reg. E clearinghouse to track and respond to attacks. The Fed should sponsor a technical committee to create an ISO specification for the initiation of payment from electronic payment devices (and traditional POS devices).

**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 payment 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 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?

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

**Response**

Central Banks must create small value gross real time payment system (SVGRTPS).

 "The "Others" are yanking your chain. The system is evolving in quite a different way, toward private banking interests rather than the public interest. It requires a public authority because the guarding of interchange fees prevents the industry from implementing a small value gross real time payment system. Acquirers and issuers make their living with the expensive and slow system now in use. Therefore, the only way to create the desired outcome is for the Fed to offer the service with its brethren central banks.

**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 U.S. near-real-time system?

**Response**

The elements stated are necessary elements.

Other good features include:

- The receiver does not need to know the sender's financial details such as bank account

- Reasonable expectation of privacy (Governments need subpoenas to look at transactions)

- Changes to Reg. E

- Alternatives for rural, badly equipped populations

- Redundancy

- Key management

- Generation of keys from personal electronic devices immune from lunch break attacks

**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 systems. This option may require a new front-end mechanism or new rules that would provide near-real-time confirmation of good funds and timely notification of payments to end users and their financial institutions.

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.

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.

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

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

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.)

**Response**

i. SVGRT.

ii. All others are riskier than a small SVGRT because of the time lags between clearing and settlement. A differed netting system is still a differed netting system regardless of its periodicity.

iii Settlement to the RFI in near real time is essential.

iv. Discrimination about the users of the system are unworthy of the Fed.

As stated earlier the only way to get the desired system is for the Fed to implement and maintain it. Current providers of card systems will not abandon their revenues.

However, there are other requirements besides speedy clearing and settlement. Payment systems need a common clearinghouse where vendors and buyers declare frauds. All reports of fraud need to be tracked so frequent abusers of the system receive the attention of local law enforcement and the removal of the participant's privileges to use the system.

Deferred netting systems such as ACH inherently need time to settle transactions and the time lag increases risk to an intolerable range.

The use of a PIN in debit transactions reduces the risk of fraud however issuers are reluctant to use PINs in CNP transactions. There are some excellent ways of entering PINs into personal electronic devices such as sending the screen location of a number randomly displayed to a cardholder and not the number the user selected. However, the growing scourge of CNP fraud cannot be deterred by PIN entry alone. If a card is not present in the transaction, then the card number should not be present either. The use of a gross real time payment system for small value transactions eliminates financial details revealed to parties other than the FIs involved.

FIs may not be able to receive a payment and immediately deposit it in the beneficiary account in real time. However, funds should leave a sender's account immediately and routed to the beneficiary account in real time. The use of the NOVUS VOVUS mechanism within a gross real

time payment system eliminates the need for a clearing function. FIs will prevent the push of unavailable funds in a variety of easy to implement methods just as they do today with Fed Wire.

**Q7**. Some industry participants have said that efforts to make check payments easier to use, such as by enabling fully electronic payment orders and/or by speeding up electronic check return information, will incrementally benefit the payment system. Others 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?

**Response**

I fully agree with enabling fully electronic payments from demand deposit accounts.

A paper check can be used to push money into the payment system, but can be thrown away after that. Buyers using checks reveal their financial data and therefore liable for the increased risk to their account. Any system should accommodate different methods to initiate a transaction and the payment system should not limit consumer choice of initiation methods.

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

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

**Response**

The method proposed reduces the exposure of financial data to the initiator and the trusted environment of the Fed Reserve and its member FI. That eliminates all but certain type of fraud. For example, it will eliminate CNP fraud, but will not eliminate identity theft. Applications running on personal electronic devices must have standard security functions such as:

- Ensuring the application has not been changed since introduction into the device
- Ensuring the application ports are not monitored by another application
- Ensuring the financial data moves to the Fed portal (acquiring node)
- Generates cryptographic keys based on the user current transaction velocity, current originating location, using Schrödinger equations.[2]

Current retail systems generally work as seen in Figure 1.

---

[2] I will be happy to show the Fed a paper I wrote but not published entitled "The Benefits of Measuring Transaction Quanta

**Figure 1: Clearing of Payment Card Transactions**
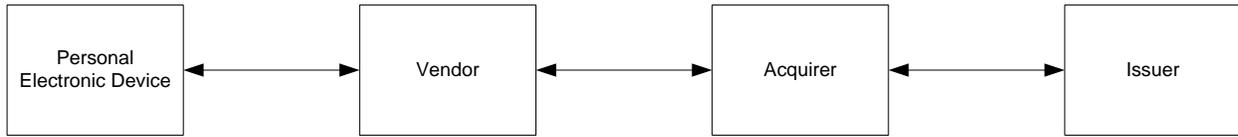


Transactions spend a long time in a non-trusted environment subject to increasingly sophisticated attacks. Figure 2 shows the reduction in vulnerability.

**Figure 2: Small Value GRTPS**



Essentially the system depicted in Figure 2 eliminates all fraud except for identity theft, strong-arm robbery, or friendly fraud. The fraud clearinghouse will help prevent repeat identity theft attacks.

Currently payment card users enjoy the full protection of Reg E. There would be no need for Reg E protection, however FIs may want to reimburse their customers in cases of strong-arm robbery or the theft of a user's buyer ID and verifying data (finger print, PIN, etc).

Another method for reducing fraud would be validating the customer's device so that a buyer ID number would need to originate from a device given to the Fed during registration time. A buyer stipulates that only payments originating from that particular device (or devices) are legitimate. As a further protection, the Fed should ensure that there is only account number associated with a buyer or vendor ID. An attempt to register an existent account with a new ID (buyer or vendor) will fail.

The current methodology for detecting fraud (neural nets) can be easily defeated. Examining the quanta of transactions and creating behavior detection filters and evasion detection filters[3] will be more effective.

---

[3] Terms developed in a talk to the EBT Directors of the New England Governor's association in spring of 2006. Speech is available on request.

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

**Response**

If people knew their personal electronic devices could initiate transactions as securely as pulling cash or cards from their wallet in their purse or pocket, then a true revolution in retail payment infrastructure will occur. Shoppers for instance, may scan a product UPC and transmit payment for it. Such a system may eliminate the cashier function for retailers. It would be a scary world for the provider's of POS equipment, because such a system may make them obsolete (the few Luddites like me that do not have a mobile phone would need an electronic check and an in-store scanner). These transactions would not receive a CNP surcharge, thus lowering transactions costs for most retailers. Users would trust the Fed with their data instead of the wary apprehension of providing financial firms with vulnerable personal data. The Fed may offer functions such as applying sales tax to the price based on location and forward the tax payment directly to the Government applying the tax. Firms would reduce their accountant costs sharply. In short such a ubiquitous SVGRT system would not just bring pivotal change to mobile payments, it would make mobile payment the preferred method; cards and cash would be left at home.

**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?

**Response**

If the Fed does not build and operate the system, no other entity will do so. We know this to be true, because the industry wants to adopt EMV, which does not prevent CNP fraud, increases the cost of transactions prohibitively, and still does not prevent data intercept attacks. The industry has expressed few initiatives to create a gross real time payment system, because there is no money in it for them; there is a lot of money for operators and bank transaction companies for implementing EMV including moving the liability to vendors. The cost of implementing the archaic EMV payment system will be in the 10s of billions, far more than implementing a SVGRT and vendors and consumers will pay those costs. The industry has a conflict of interest with a SVGRT and will do everything in their power to prevent its introduction in the US.

**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?

**Response**

No modernization is necessary, use the same methodology currently used for Fed Wire. Start with that, offer it immediately and the industry will introduce all types of innovative ways their customers can use it. Work on better ways to detect and deter fraud and the payment industry will cooperate fully and use technology to enhance the services to their customers.

**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?

ii. What is the feasibility of this suggestion?

**Response**

-The critical part is the payer pushes the payment onto the platform and it determines the debit account, the credit account, and the route for the transaction. The other critical part is the trusted nature of the platform, without the trust, the design will fail. The payment system industry will create many ingenuous ways to implement the backbone and access to it. An LDAP solution is one of many good solid approaches.

**Q13**. Some industry participants say that check use is an enduring part of the U.S. payment system and that moving away 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: "By the year 2018, 95% of all noncash payments will be made via electronic means."

iv. What is the appropriate target level and date?

**Response**

i. What is the hurry? Consumer choice of payment initiation allows alternatives to the digital age. Until you can say that all vendors are required to have phones or internet, electricity, and an electronic link to a payment system, you cannot force users to abandon methods that have worked well enough. Also it is good to have alternatives if the lights go out.

**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?

**Response**

**i.** Firms make money on the float. Until the cost of writing a check costs more money net than using an electronic payment system, checks use will dwindle at its current (or reduced) rate.

**ii**. Consumers and firms need ubiquitous access to E-check conversion by consumers. Imagine a banking application resident on a personal electronic device that takes a picture of a check and the amount shows up in the payee account within seconds, as cash (or bounces). The unbanked will not receive the benefits, but every suffering small business, handyman, or moonlighter will dance with joy from the speedier cash flow.

**iii.** Encourage use of depositing funds by e-check reduces the float, and reduce incentives for using checks.

If you build a SVGRT, then businesses will use it instead of ACH or checks. As a small business, I cannot use ACH because it is cost prohibitive. I have used QuickBooks for payroll that in turn uses ACH, but for me to get my bank to offer the same service is a fool's errand. FI do not listen to small business requests for functionality, and so if the service does not exist, consumers cut checks.

**iv.** I am not sure, perhaps a combination of NACHA, the FED, and others.

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

**Response**

ISO 20022 was designed for payment versus demand payment systems but is remarkably versatile. Since it uses HTML tags instead of the dreaded bit maps of ISO 8583 more people can readily write applications in modern programming languages using the format. If the industry continues its current clearing structure then replacement of ISO 8583 with ISO 20022 makes sense since programming, analysis, research, and back end processing will not require using a format that is hard to parse and use in a constructive manner.

However, making a reasonable change to an internal format will not increase the rate of demise of checks. Asking the owners of businesses that use ISO 8583, if it makes sense to do it, then panic over the amount of changes that will need to be made to existing applications, the consequences of failure, and the costs needed to make the change, will prevent ISO 20022 use in retail clearing systems.

In today's world, there is no real need for acquirers, terminal drivers, POPs, or proprietary financial networks. ISO 20022 allows the smallest of businesses to create an ISO 20022 request and send it by internet directly to the issuer for approval. In that way the reduction of costs processing transactions may increase the use of electronic clearing processes from the point of sale.

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

**Response**

Small value gross real time payment systems.

**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?

**Response**

Interception of financial data, be they in flight or at rest, and the subsequent unauthorized use of that data is the modi operandi of most thieves. We see that in skimming attacks, and database attacks in the US, and the intercept of wireless messages in retail establishments in Britain. The

recent attacks on authorizers in India used a different approach, the increase of fund limits associated with particular cards.

The vulnerability of CNP transactions (EMV or otherwise) remains the low hanging fruit for attackers and the industry response to it is dismal at best. The loudest response is that the US must adopt EMV and then all their problems will go away, when EMV does nothing to address CNP fraud.

The industry can take two actions to reduce CNP fraud, namely:

- Authorizers must validate that the origin of a payment request is equipment registered with the cardholder
- Establish an international fraud clearinghouse to record and analyze all Reg. E claims.

Other actions such as authorizers having velocity limits on account access and the use of neural nets helps somewhat, but thieves know how to avoid these old solutions.

I would be glad to discuss effective ways to combat fraud with techniques I mentioned briefly earlier such as generation of keys from payment quanta and behavior detection filters/evasion detection filters based only on the data within the transaction, however I do not want to discuss these concepts in a public forum.

**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?

**Response**

All attacks (successful or not) need to be registered in one international location where the data can be analyzed. The activities of this clearinghouse should be mostly secret except to announce new types of attacks and prevention of attacks. The lack of such a clearinghouse means that Reg. E claims against several FIs do not have their common elements revealed and so the attacks continue, until there are common elements from differing Reg. E claims within the same FI. The G10 central banks could easily build and operate such a fraud clearinghouse.

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

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

**Response**

The following standards would increase the security of transactions:

- The geocode of the equipment originating the transaction

- Identifying data of the equipment originating transactions
- Secure use of PINs in all transactions

Obstacles to these standards mostly arise from the industry not critically thinking about the attacks currently in use but instead believe the solution to fraud generally is to increase the sophistication of payment tokens and processing equipment; development which does nothing to prevent the actual attacks occurring.

**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?

**Response**

As discussed earlier the Fed should create:

- A small value gross real time payment system
- An international fraud clearinghouse

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

**Response**

I have many ideas on how to improve the payment infrastructure; however, I do not want to share them in an open forum. I am willing to share them with people or firms willing to sign a non-disclosure agreement with me.

Ed Oppenheimer

Edward.Oppenheimer@ThoughtMatrixConsulting.com

703.476.8778