Gray Taylor
Executive Director
Petroleum Convenience Alliance for Technology Stds
1600 Duke Street
Alexandria, VA 22314

December 13, 2013

Ms. Sandra Pianalto
President and CEO
Federal Reserve Bank of Cleveland

Dear Ms. Pianalto:

The Petroleum Convenience Alliance for Technology Standards (PCATS) is pleased to respond to the Federal Reserve Banks' (FRB) "Payment System Improvement – Public Consultation Paper" and is appreciative of the opportunity to participate in setting the payments objectives of the Federal Reserve Bank. PCATS agrees that payment systems are in need of modernization and competition. Efficient payment systems are essential to a healthy and competitive national economy, and PCATS believes it is imperative that our country focus on regaining world leadership in payments through productivity and innovation in payments.

PCATS is a non-profit standards organization representing the 149,000 convenience and petroleum stores operating in the U.S., and the technology, consumer goods and services suppliers that serve the industry. Since 2003 over half of our industry's fuel sales have been transacted on card systems and the industry has seen its total cost of card payments soar from $3.3B in 2003 to $11.2B in 2012 (the first full year of Durbin price impacts).

Since its inception in 1996, PCATS membership has focused on seamless and standardized integration to the industry systems of all viable payment alternatives, clarifying data security best practices and more recently, standardized methods of integrating mobile commerce solutions. As part of its work, PCATS is involved with other, accredited standards bodies such as ANSI X9 and the World Wide Web Consortium, in an effort to incorporate existing public standards wherever possible. This commitment to accredited standards led to PCATS releasing the first use case standard for point-to-point encryption, based on the X9 standard.

PCATS also participates in non-accredited guidance organizations such as PCI and the EMV Migration Forum, in order to best advocate for the needs of our membership, and decipher the often times confusing mandates of the card brands. In addition to card brand security mandates, PCATS has led the

pan-retailer effort to materially reduce payments security risk through a series of “Guides” that help retailers reduce risk, rather than focus on card brand compliance.

Please find attached our summary responses to the consultation paper. PCATS stands ready to assist the Federal Reserve in its admirable objective of bringing efficiencies to the payments markets.

Best Regards,

Gray Taylor
Executive Director

PCATS Comments to Consultation Paper

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

PCATS is in general agreement with the gaps and opportunities outlined by the FRB. Secure real-time payments are of particular interest to PCATS. As consumers continue to rapidly adopt mobile commerce/computing, continued failure to demand corresponding payments efficiencies and security will stifle this innovation to the detriment of our national competitiveness.

There are no technical barriers to real-time payments, but PCATS understands that moving the world's largest economy to state-of-the-technology will take time and investment – and intermediate steps such as near real-time solutions should be implemented in the shorter run. PCATS therefore generally views short term enhancements to ACH – near real-time transactions, fully authenticated at time of initiation, with funds availability verified – as a paramount near term strategy for our economy.

Longer term, and possibly with the abandonment of the current ACH and card payments design, real-time payments should be our country's objective. Adoption of US standards to accomplish this goal would be the best outcome; ANSI X9 has a proven track record of developing standards for the US financial industry.

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

PCATS believes that the lack of financial institution interest in changing the existing system due to lack of financial or regulatory incentives is a significant gap that must be addressed if the Federal Reserve Bank is to achieve its admirable goals.

PCATS also wishes to clarify gap point 8, in that survey after survey of consumers shows not a fear of payment security – that is largely assuaged by Regulation E and as an enticement to private payment systems through cardholder agreements. Consumers are fearful of identity theft, which is not indemnified by any institution or agency, and exploited because of archaic identity authentication in the digital age. Rather than share liability with consumers, PCATS believes this gap should focus on authentication of identity in payments. Here, again, X9 standards should be used as the mechanism for achieving this result.

PCATS also believes that the objective of completing secure transactions in less than secure environment be identified as an opportunity of the Federal Reserve strategy. Current systems assume that the processing environment is "pristine" and free from intrusion, which has led to billions of dollars in participant investment to pursue, what should be assumed, an impossible goal of keeping the payment system free of intrusion. By assuming that future systems will not be impervious to penetration and focusing on how to authenticate valid transactions – "clean data in a dirty world" – should be a guiding principle of any future strategy.

Tokenization and encryption, when combined with strong authentication, allow valid transactions to occur in even the most porous data environments, as an example. In this arena, X9 has recently adopted X9.119-Part 1 dealing with point-to-point encryption;

standards development work is underway on tokenization (X9.119-Part 2). This works, should be encouraged and all interested parties should be encouraged to participate in its completion.

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

Desired outcome 1 states "collectively identified and embraced by payment participants". PCATS wishes to stress that the definition of "participants" be understood to include non-financial participants, including, but not limited to, retailers, merchants, government and the general public.

Desired outcome 3 states "end-to-end (societal costs)". PCATS wishes to stress that this definition include direct and indirect costs relative to payments, whether charged directly to a participant or indirectly through another participant.

Desired outcome 5. PCATS believes that the worthy objective of Outcome 2, "A ubiquitous electronic solution(s) for making retail payments exists that does not require the sender to the bank account number of the recipient" cannot be adequately achieved without the security provided by improved generic identity authentication leveraging currently available technologies. Further, that national security interests around improved identity expand the need for enhanced identity authentication that would naturally seek to leverage the method(s) resulting from this strategy. PCATS believes that the Federal Reserve Bank must lead – not only collaborate in - this discussion and incorporate other governmental agencies to ensure a ubiquitous and secure identity authentication system(s) for societal use.

i. What other outcomes should be pursued?

None at this time, but PCATS fully expects additional opportunities will arise with this process.

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

The Federal Reserve's leadership in ACH is an excellent example of how its participation in the payments system can foster profitable efficiency in the market. As with ACH, where systemic innovation is desired, we believe that the Federal Reserve should provide a baseline system as an example and resource for FIs to quickly adopt the new paradigm. ACH has proven that competing systems can flourish without pricing distortions brought on through market powers.

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 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?

PCATS believes that regulators should seek to promote market force influence in payments migration through:

- **Requiring that all pan-economic payment systems data format and security rules be standardized in accredited standards bodies, and**
- **Account holder privacy be required and protected through full authentication of identity, again set by accredited standards bodies, and**
- **No private entity(s) be allowed to control the methods of authentication of identity, and**
- **That no financial institution will unreasonably restrict account access of any payment method that adheres to the above.**

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

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.

PCATS agrees with the stated features. PCATS believes that, in more simplistic terms, digital transactions should ultimately approximate cash transactions in their use and timeliness.

ii. What other characteristics or features are important for a U.S. near-real-time system?

Payer should be the initiator of near real-time transactions upon presentation of an invoice or statement as a base feature, much like cash or check transactions. There will be instances, such as recurring payments, where the receiver will initiate the transaction, but this is secondary in importance to retail.

As an example, why would it not be more secure and efficient if a retail customer would be presented the invoice (electronically) to their mobile device, and the customer merely authorizing payment to that merchant of the invoice amount. The invoice number and merchant receiving information is the only data exchanged at the sale, with finalization of the sale coming from receipt (or guarantee) of payment received by the merchant. At no time was any customer data be exposed, payment advice to the FI was suitably authenticated and encrypted, processed by the FI in a secure data center, and advice forwarded to the merchant.

This method is the cornerstone of innovative systems offerings such as MCX and PayPal.

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?

Modifying the existing ACH system; pushing its capabilities beyond "same day" to at least multiple batch settlement with real time funds validation and strong identity authentication (capable of bridging to online retail transactions). In this vein, the FRB has existing authority to lead and mandate changes to ACH as a matter of "check" clearance efficiencies; to clear voting block pushback by those few FIs in ACH associations who seek to preserve interchange revenues at the expense of ACH efficiency.

PCATS believes that modifying the ACH system would be a near-term goal, with the longer term goal being true real-time payments with secure authentication, which may or may not be able to be achieved on the ACH system.

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?

Creating a new wire-transfer like system would require much of the same FI investment as leveraging a more robust ACH network, but would require yet another settlement system. PCATS believes this alternative only viable if modifying ACH proves more disruptive or expensive.

Enhancing existing debit card networks – along with modernizing identity authentication – presents the second best choice in PCATS' opinion. Distorted interchange pricing queues found in these systems is the largest disqualifier of this option, as the incentives are for FI revenue and not efficiency.

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?

Near real-time settlement of funds is secondary to near real-time authorization, authentication and settlement advice, so long as all three of these features are present and settlement occurs several times per day.

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

P2P in an open loop payment system is probably least viable, assuming that consumer is least likely to implement a reliable platform, or choose between the myriad of platform offers (e.g. mobile wallet). The proliferation of limited participation networks also works against P2P viability, as network interaction cannot be assured today.

Where one side of the transaction has payment volume, such as B2B, POS or P2B, it can be assured that at least one party will have sufficient infrastructure to affect a reliable transaction.

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?

Assuming that the "end game" is a more efficient payment system, PCATS agrees with the latter statement in Q7. Current efforts to replace checks with digital payments are varied in capability, lack a coordinated "directory" of participants (especially persons) and are generally expensive for small business or individuals to implement. Most current iterations of personal digital payments tie the consumer to the FI, forcing the consumer to "rebuild" their payee list when they change banks.

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.

Without improved authentication, near real-time will falter due to fraud, as the ultimate fraud control – the account holder – will not be able to respond to a breech in near real-time. The risk of significant fraudulent withdrawals occurring before the account holder notices is heightened with near real-time, without vastly improved authentication to offset this new risk. Existing velocity controls in the card payments markets are ineffectual, as a result of liability shifts present in the card markets; this problem represents a further barrier to true identity authentication.

Limited participation networks, because of their small scale, have not begun to experience the true risk of today's implementations.

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

Near real-time would fulfill the missing promise of mobile banking – that the mobile user has true access to their funds, and that the balance displayed on their phone is not potentially encumbered by pending transactions. It would create a true digital asset account without ledger and available balances, which would complement the real-time nature of mobile commerce.

Authentication advantages of mobile devices will also reduce fraud risk with the simple validation of the device as a valid "card" – even for use in online purchases. Further authentication of the user will only strengthen the security of the system, making the system superior to existing technology

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?

Failure to fully act on *all* required items for an efficient payment system will be a significant competitive disadvantage to the US economy, especially when key trading partners, like the UK, are pushing into more efficient payment systems. The latent friction of the existing system will only become more obvious as other markets migrate to real-time and near real-time systems.

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?

Some modification in retail treasury and payment would be expected to accommodate intraday debits and credits, and away from daily batch processing. POS modifications – already in standards process to accommodate mobile commerce – will also need to be implemented.

To be clear, speed to market of any innovation will have to include the premise of "better, faster and cheaper" in its premise, or risk significant delays.

Total industry time lag is greatly dependent on ROI inherent to any payment innovation. If cost efficiencies are great, and shared with retail, the "time to market" will be greatly expedited; with less than 2 years a reasonable estimate. If the ROI to retailers is significantly less than 25%, implementation will be much longer and tied to normal IT upgrade cycles or not at all.

EMV migration is an excellent example of how the lack of economic benefit will retard deployment. PCATS membership *has no financial incentive* to concentrate capital on EMV even with the "stick" approach of liability shift.

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?

A "tokenized" identifier is only critical where enhanced identity authentication is not used, as the account and routing/transit data become vulnerable to fraud with easy access. Where identity authentication is strong, then exposing the actual account and routing/transit becomes much less a security issue with corresponding reduction in need for tokenization.

PCATS believes that an easy method of determining receivers of electronic payments would facilitate P2P and P2B segment adoption.

ii. What is the feasibility of this suggestion?

Participation (both use and enlistment) would be potentially driven by cost, reduction of float and independence from FIs as intermediaries. One risk to be addressed is that such a system could be used as part of an account takeover scheme, which would be greatly mitigated through secure identity and/or trusted service provider provisioning of records.

Electronification

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.)

Yes, if the electronic payment system of the future is indeed more efficient. In today's environment, checks with truncation are much more efficient than payment cards at retail, as mentioned above.

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."

No comment

iv. What is the appropriate target level and date?

No comment

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?

A core impediment to retail adoption of digital payments is State requirements surrounding certain vendor payments (such as alcohol and beer) that do not recognize widely available methods of check replacement; like ACH or even checks themselves. The lack of State recognition of ACH forces retailers to use money orders or payment guarantor intermediaries to meet State rules of immediate payment.

State recognition of ACH and other near real-time payments is essential for retail B2B payments completely moving away from checks.

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

As mentioned above, sharing of efficiencies with stakeholders and a comprehensive directory of near real-time payment participants is needed to extend digital payments to low incident or one time payments made by both business and consumers.

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

Public education of the benefits and security of near real-time payments is essential.

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

Retailers will always – where allowed – steer consumers to the most efficient method of payment. Should near real-time payments offer distinct savings and other advantages, retailers will naturally educate consumers at the point-of-sale. However, this ability to steer is limited to the relative cost of payments choices, which increasingly is diminutive as debit alternatives approach (and even exceed in small ticket transactions) the cost of credit cards.

Financial institutions should have a vested interest in reducing their costs of account management through going "paperless". It is reasonable to expect FI's to educate, and even

incent, their customers to the lower cost payment methods as a matter of self-interest However, if the result is a lowering of revenue as customers adopt "less than interchange" payment alternatives, education will be absent and financial disincentives – as have been introduced in PIN debit markets – should be expected.

Cross-border payments

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?

This would technically resolve the translation problems in existence today, but currently has the practical issue of ISO 20022 not supporting our existing message type (ISO 8583). This issue is already being addressed by ANSI X9.

PCATS believes that the Federal Reserve should leverage its existing participation in ANSI X9 to all standards setting in financial payments. In doing so, the FRB is fostering the open participation of all stakeholders in the payment ecosystem by example.

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?

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?

As mentioned previously, PCATS believes that identity authentication is the cornerstone of any secure payment system; today in card payments and in future payment systems.

PCATS believes that payment account information, inadequately protected in today's system, is too distributed to consumer touch points that cannot be reasonably assured secure. This design flaw in the current system incents criminals to compromise the distributed endpoints to gain access to the customer accounts flowing through that endpoint, and places merchants in the untenable and hopeless situation of protecting those endpoints in support of an outdated system. In this respect, critical data is always best kept in central secure servers, under constant surveillance, limited access and with capable security systems, or (less desirable) on a personal device where the fraud opportunity is confined to an individual.

PCATS also believes – as mentioned above - that the current method of "pulling" payment from a customer account, as currently practiced in retail payments, is inherently flawed and a product of archaic technological barriers. ACH security studies indicate that the vast majority

of fraudulent transactions are "pulled" from accounts, with "push" transactions rarely subject to fraud (except in cases of account takeover).

PCATS cannot stress enough that its desire that the Federal Reserve Bank will take a "fresh eyes" approach to payments, recognizing that a "pushed" transaction by a fully authenticated account holder to a payee is far more secure than trying to improve the current "pull" system. That while the consumer should not bare the entire risk of the system, the consumer must become a stakeholder in his or her own identity in the digital age – a responsibility largely obfuscated in current payment systems.

ii. Which of these threats are not adequately being addressed?

None of them are being adequately addressed in the current system.

iii. What operational or technology changes could be implemented to further mitigate cyber threats?

User controlled and owned secure digital identification (provided by a highly trusted service provider) should be the primary focus, as only with strong authentication can secure transactions be conducted in less than secure data environments; which, as mentioned before is the reality of distributed payment systems. "Hard-to hack" credentialing would allow all other data could transmit "in the clear" with little risk of compromise and resultant fraud. This reduction can be expected as a critical and dynamic piece of data required to initiate a transaction is unavailable.

The consumerization of mobile computing devices offers a critical ally in providing secure identity authentication, in that these devices can produce highly encrypted authentications, while lessening the "value" of compromise as the device is a) difficult to breech (potentially) and b) represents only one consumer account.

Urges the FRB to recognize that this secure identity, if truly secure, will also be used for other identity needs, such as licensing, secure access, medical records access or proof of citizenship, and a holistic approach from government agencies will need to be coordinated; that this is not a card brand or social media exercise. Wider use of secure identification should be comprehended in any strategy to improve payments, primarily as multiple use cases will only serve to multiply consumer value and uptake.

In the current state and in contrast to PCATS' proposed end state, sensitive data flows en masse in data pools that cannot be reasonably secured, offering both insecure data and large pools of accounts. Again, PCATS cannot stress enough the criticality of *assuming* that no transaction network will be immune to penetration, and therefore focus must be on making the transaction immune.

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?

There already exist forums and databases to adequately warn of threats and trends, but always room for promotion by government agencies. In fact, PCATS operates an industry incident database for its membership.

A significant barrier to full exploitation of incident reporting is the very real threat of retribution by regulators – both public and private – in response to a system stakeholder's timely reporting of an incident. The practical risk of the breeched victim again becoming a victim of fines, sanctions and lawsuits often causes a significant delay in reporting critical and timely data until legal protection has been secured. PCATS recommends that "whistleblower" like protections be offered to stakeholders reporting early and fully for the benefit of the entire payment system.

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

PCATS strongly believes that the operant term is "standards". A word that is all too often used inappropriately by those imposing private specifications as mandates, true standards are derived by all stakeholders in a system or market to achieve efficient and implementable interoperability and processes, in a setting where the standards organization governance is open to all stakeholders. Privatized payment systems selectively combine true standards generated by accredited organizations such as ISO or ANSI X9, with privately generated "standards" from non-accredited organizations governed by card brands.

PCI and EMV, sold as standards bodies, are primary examples of this misuse. In fact, they are organizations designed to enforce the collective wills of the card brands.

In an optimal scenario, ALL payments data formats, processes and structures would be determined in a fully accredited standards body, such as ANSI X9 in the US. The advantages to society of such a process are manifold. First, all stakeholders would have an opportunity to materially shape an equitable and market-derived payment system. Second, innovation would be freed of individual stakeholder interests, allowing the best state-of-the-art payment systems attributes to come to market. Third, adoption rates would reasonably be expected to accelerate, as all stakeholders have ownership in the system.

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

Market domination by the card brands, with corresponding monopoly profits, are the sole barrier to significant adoption of security-related standards. In today's system, merchants fund a disproportionate amount of securing private payment systems.

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?

PCATS believes that the Federal Reserve should provide leadership of a public/private initiative with regulatory teeth. Oversight of payments is a matter of consumer safety and national security and, as such, should rely on private enterprise being given the opportunity to work out the optimal societal solution to payments security, but with the understanding that, like any consumer safety issue, consequences for inaction or non-compliance are in place.

It is absurd that state and federal regulators are increasingly looking to organizations such as PCI to be the arbiter of security standards, and to continue to allow the card brand owners of this organization to use "fines" as if they were duly authorized public regulators.

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