W. Capra
CONSULTING GROUP

221 NORTH LASALLE ST. | CHICAGO, IL 60601 | 312-873-3300 | INFO@WCAPRA.COM

Managing Risk in Faster Payments Systems

An examination of the Faster Payments Task Force and associated risks of the Faster Payments Proposals

Published November 1, 2017

Introduction

The existing US payment infrastructure has not kept pace with the rate of technological advancement. The complex infrastructure of the US payments system, driven by the considerable number of relationships between its stakeholders – government institutions, financial institutions, payment systems, merchants, consumers, and service providers – has induced a slower pace of financial innovation than that of other countries. The Faster Payments Task Force ("FPTF") looks to change that by identifying a roadmap for modernizing the US Payments system.

The U.S. Federal Reserve assembled the FPTF with the mission to "identify and evaluate alternative approaches to implementing safe, ubiquitous, faster payments capabilities in the United States" [1]. The scope of this task force includes the end-to-end payment process including authorization, verification of the availability of good funds to payee, settlement among both depository institutions and non-bank account providers, clearing, and visibility of payment status throughout the value chain. In addition, all types of end users are to be considered including consumers (banked and unbanked), businesses, service providers, and government entities.

The FPTF designed a 5-step approach to facilitating the conversation and innovation within the payment industry. Figure 1 below outlines this approach.

Any new electronic payment system assessed and agreed upon by the FPTF must be able to instill confidence in individuals, businesses, and governments alike to drive adoption. It is imperative that any new system incorporates and improves upon the existing safeguards that our current payment systems have in place to provide safety and security for all participants at every step of the payments value chain. The opportunities created by the instantaneous movement of money around the world will also create new challenges and risks that all transaction participants must be able to address for any new payment system to succeed.

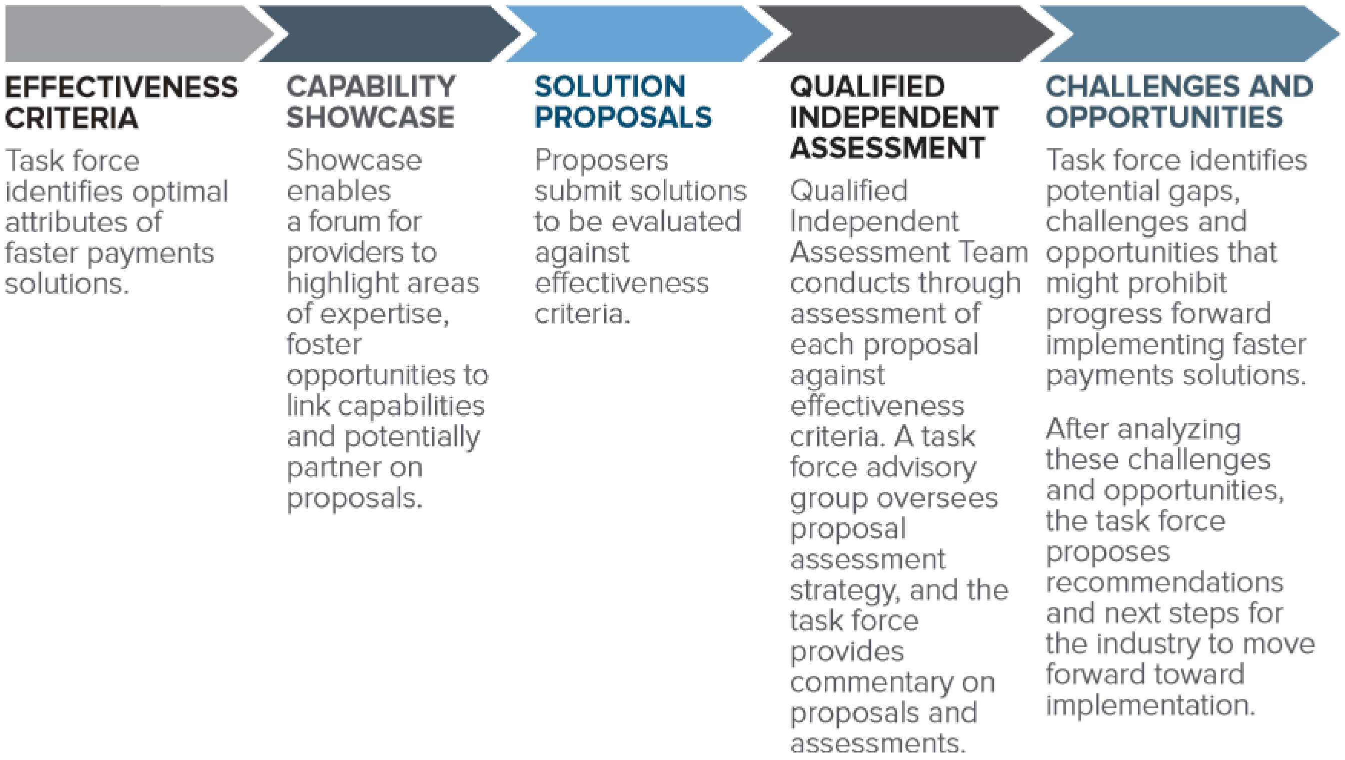
In order to provide the required assurance of individual payment transactions, we identify three core functions that must be appropriately performed by one or more system participants:

- *Authentication:* The ability to authenticate the payment credential that is being used.
- *Verification:* The ability to verify the individual initiating the transaction is indeed the account owner (or an authorized user).
- *Authorization:* The ability to validate the availability of funds and transfer them to the counterparty in the transaction.

In addition to assuring individual payment transactions, electronic payment systems must also maintain the security and operational integrity of any new system to ensure participant trust in the systems. Alongside traditional cybersecurity protections, it is critical that electronic payment systems implement stringent controls for:

- *Data Security:* Protecting sensitive data in use, in motion, and at rest.
- *Operational Integrity:* Preventing full or partial disruptions to system operations caused by malicious actors.

These five functions (Authentication, Verification, Authorization, Data Security, and Operational Security) represent controls critical to the success of any electronic payment system. The focus in this work centers on how these risks controls are implemented within existing payments systems and subsequently on how these risk controls could be applied to proposals being evaluated by the FPTF.



EFFECTIVENESS CRITERIA
Task force identifies optimal attributes of faster payments solutions.

CAPABILITY SHOWCASE
Showcase enables a forum for providers to highlight areas of expertise, foster opportunities to link capabilities and potentially partner on proposals.

SOLUTION PROPOSALS
Proposers submit solutions to be evaluated against effectiveness criteria.

QUALIFIED INDEPENDENT ASSESSMENT
Qualified Independent Assessment Team conducts through assessment of each proposal against effectiveness criteria. A task force advisory group oversees proposal assessment strategy, and the task force provides commentary on proposals and assessments.

CHALLENGES AND OPPORTUNITIES
Task force identifies potential gaps, challenges and opportunities that might prohibit progress forward implementing faster payments solutions.

After analyzing these challenges and opportunities, the task force proposes recommendations and next steps for the industry to move forward toward implementation.

Figure 1. FPTF Approach to Faster Payments [1]

Analysis of Traditional Payment Systems

US consumers and businesses rely upon the four traditional payment methods to exchange funds for goods and services:

- Cash
- Check
- Card (includes credit, debit, pre-paid, etc.)
- ACH

Each of these payment methods represents "transactional systems" for recording events and transmitting value: Payer presents tender to payee in exchange for goods/services, and payee – leveraging information provided by banking institutions – determines the validity and account sufficiency of the tender presented.

Data in such transactional systems is shared primarily between the payer and payee, and – in the event of electronic methods – the payer's representative banking institution, the relevant system providers (e.g. VISA), and the payee's representative banking institution.

The acceptance of each transactional payment method is characterized by a particular set of risks related to the core functions outlined in Section 1. Over time, the systems for accepting these traditional methods have implemented controls to reduce the exposure these risks pose. Table 1 outlines these risks and examples of corresponding controls that have been implemented for each of the traditional payment methods listed.

Table 1. Risk Analysis of Traditional Payment Methods

	Type	Risks	Examples of Controls Implemented
Authentication	Cash	Counterfeit physical currency	• Payee/merchant validates the authenticity of currency • Utilize services to detect the presence of anti-counterfeit devices in currency
	Check	Counterfeit or tampered checks	• Payee/merchant validates formatting, spelling, incorrect or missing MICR data • Validate routing number to ensure correspondence to correct FI on check
	Card	Counterfeit cards/accounts	• Validate authenticity of physical card • EMV (chip card) issuance and acceptance
	ACH	Counterfeit accounts	• Pre-notes ($0 deposits) and micro-deposits (small deposits validated by consumer) • Out-of-band, credential-based authentication with customer's banking institution
Verification	Cash	None	• No applicable controls
	Check	Forged signature	• Validate customer's identity against another form of identification • Use of check acceptance and warranty/guaranty services • Collect customer's signature on receipt for dispute protection
	Card	Lost/stolen cards	• Validate customer signature or PIN entered by customer • AVS, CVV and 3D-Secure (Verified by Visa, MasterCard SecureCode, etc.)
	ACH	Account takeover	• Validate customer access credentials • Multi-factor authentication ("MFA") methods in conjunction with banking institution applications
Authorization	Cash	None	• No applicable controls
	Check	Insufficient Funds	• Customer's bank makes funds available via overdraft loan • Check returned to the merchant for re-presentment
	Card	Insufficient Funds	• Online authorization to verify funds availability • If sufficient funds available, customer's bank places authorization hold for order amount to ensure payment to merchant upon settlement
	ACH	Insufficient Funds	• ACH processing provider may guarantee funding up to certain dollar amount threshold
Data Security	Cash	None	• No applicable controls
	Check	Theft of account information	• Transportation-layer encryption of electronic check processing • Secure storage and destruction of physical checks
	Card	Theft of account information	• Application-layer encryption of card account details during processing • Transport-layer encryption of card processing transmission • Irreversible tokenization of card account details when storing for future use
	ACH	Theft of account information	• Transportation-layer encryption of transaction messages • Encryption of account details when storing for future use
Operational Integrity	Cash	Theft	• Cash counting and automated deposit services
	Check	Electronic check service unavailable	• Implement rate limiting to protect applications from Denial of Service ("DoS") attacks • Monitor traffic for known bad device signatures and anomalous message volumes
	Card	Card processing service unavailable	• Implement rate limiting to protect applications from Denial of Service ("DoS") attacks • Monitor traffic for known bad device signatures and anomalous message volumes
	ACH	ACH processing service unavailable	• Implement rate limiting to protect applications from Denial of Service ("DoS") attacks • Monitor traffic for known bad device signatures and anomalous message volumes

Overview of Proposals to FPTF

As of September 2017, the FPTF received and began analysis of 16 proposals for a new faster payments system in the US. Although each has unique design characteristics for addressing identity management, security, integrity, and interoperability, the proposals can be categorized into two groups:

1. *Improved Transactional Systems:* Proposals in this category present significant improvements (funding speed, security, authentication, cost) to existing transactional systems. However, the solutions proposed in this category still perform authentication, verification, and authorization in a transactional approach, where data is only shared between stakeholders participating in the individual transaction.
2. *Distributed Systems:* Proposals in this category contemplate solutions for securely authenticating, verifying, and authorizing payments via distributed ledger systems. Transaction data is shared, validated, and accepted/declined across a designated federation of payment system participants.

The FPTF evaluated each of the 16 proposals submitted against the following effectiveness criteria [1]:

1. Risk management
2. Payer authorization
3. Payment finality
4. Settlement approach
5. Handling disputed payments
6. Fraud information sharing
7. Security controls
8. Resiliency
9. End-user data protection
10. End-user/Provider authentication
11. Participation requirements

In the following section, we analyze the categories of proposals in regard to the effectiveness criteria highlighted above. We have chosen these effectiveness criteria as they represent areas related to managing risk associated to consumer-based payments.

Analysis of Proposals to FPTF

Understanding what account authentication, user verification, and transaction authorization are, and how existing payment systems address these core functions, while still balancing the integrity and security of the network, is the first step in understanding the challenges that new payment systems will face in their design and implementation. Although we do not fully know how each proposed solution plans to accommodate these functions, we can look to the characteristics of the system type – transactional and distributed – to surmise how each can be addressed and implemented. Transactional and distributed systems each offer relative strengths and weaknesses in achieving these goals. Transactional based systems improve upon the existing framework of US payment system, offering advances in the way that information is shared between existing stakeholders in the payment infrastructure. Distributed systems, however, represent a truly new form of technology: the stakeholders, and the functions that they perform in the payment process are much different than what we would see in a transactional based system. The following table identifies how each proposal type – distributed and transactional – may perform account authentication, user verification, and transaction authorization. Additionally, the table identifies how each system can ensure data security and operational integrity.

Table 2. Risk Analysis of FPTF Proposal Types

	Proposal Type	Risks	Controls to Consider
Authentication	Distributed	Account cannot be validated on the distributed network and/or cannot appropriately interface with the requesting/receiving distributed network.	• When a customer provides a digital wallet/address, perform a check to ensure that it is a validated account on the distributed network. • Consider querying additional fields which can be used to authenticate the account, including account age, previous transaction dates, and previous transaction recipients to ensure it is indeed authentic.
	Transactional	The account information provided is inaccurate.	• Utilize a real-time account authentication measures utilizing customer supplied credentials and data linkages to financial institutions, similar to what we see with ACH today. • Create a centralized database of validated accounts that can be securely queried by merchants/payment service providers. • Consider utilizing tokenization to ensure that the customer's account can be validated without exposing sensitive information.

Table 2. Risk Analysis of FPTF Proposal Types (Cont.)

	Proposal Type	Risks	Controls to Consider
Verification	Distributed	The individual performing the transaction is not the owner (or authorized user) of the account.	• Implement identity validation by requiring the customer to "sign" the transaction by utilizing their account "private key" or by providing a validated identity token. It will be important that any credentials provided are properly managed and that the customer is aware of the impact that losing their "private key" could entail. • Merchants should also consider implementing other means of identity validation, including MFA via SMS, email, or by dedicated mobile applications.
	Transactional	The individual performing the transaction is not the owner (or authorized user) of the account	• Incorporate device-based user verification measures when initiating a transaction, including finger-print/facial recognition and MFA. • Consider implementing Password-less (UAF) and Second Factor (U2F) identity validation technology into Digital channels.
Authorization	Distributed	The funds are available in the customer's account/wallet	• A distributed network would allow the payee to query the account balance of a given account/wallet address prior to initiating a transaction. • So long as the account authentication and identity validation are successful, and the transaction meets the "rules" as established in the network, the transaction will be validated by the network participants and funds will automatically be transferred in real time.
	Transactional	The funds are available in the customer's account/wallet	• Develop and incorporate standardized payment and non-payment data related messaging capabilities to enhance transparency around funds availability. Any solution must consider customer privacy and should not expose private information. • Determine the parameters for allowing a transaction to be cancelled/reversed after initiation.
Data Security	Distributed	Theft of "keys" to access account value	• Assign irreversible token values to "private keys" when storing for funds conversion and transfer • Secure data transmission to ensure integrity of data posted to distributed ledger
	Transactional	Theft of account information	• Application-layer encryption of card account details during processing • Transport-layer encryption of card processing transmission • Irreversible tokenization of card account details when storing for future use
Operational Integrity	Distributed	Compromise of system's validation function	• Continuously monitor system performance and latency to minimize impact of validation time has on customer experience • Periodically confirm integrity of nodes within the system that are responsible for validating new transactions
	Transactional	System processing unavailable	• Implement rate limiting to protect applications from Denial of Service ("DoS") attacks • Monitor traffic for known bad device signatures and anomalous message volumes

Conclusion

The FPTF has stated that its goal is to make a faster payments solution available to financial institutions, consumers, merchants, and stakeholders alike by the year 2020 [2]. Given the complexity of the US payments infrastructure, and the vital role that it plays in the global economic engine, this is an extremely lofty, but achievable goal. The most crucial factors in meeting this deadline will be the FPTF's ability to creatively leverage new technology, while still utilizing and integrating with existing components of our legacy payment infrastructure, in order to develop a payments framework that continues to improve on the core tenants of any effective payment system – speed, security, and interoperability.

The FPTF has clearly spent time thinking about the requirements and implications of the design of a new payments system, as evidenced by the diverse group of individuals serving on the task force, and the detailed analysis and consideration that has already been performed. In addition to solutions which leverage existing components of the US financial system, the FPTF has made it clear that it is open to utilizing brand new tools, like Distributed Ledger and Blockchain technology, in order to create the fastest and most secure payment system available.

The technology utilized will be important, but the thoughtful identification of the relationships, roles, and responsibilities of the numerous stakeholders – individuals, merchants (both large and small), financial institutions, technology providers, and the government – as they interact with one another and the new payments system will be vital to the system's success. Any solution which unduly burdens or impacts one party could severely impact the adoption of the solution.

The inherent complexity of the US payments infrastructure, with its myriad stakeholders, regulations, and its rapid evolution through financial technology makes it easy to overlook the interests and concerns of individual stakeholder groups. W. Capra strongly encourages anyone who will be impacted by changes to the US payments infrastructure to become an active participant in the discussion. Only then can all the voices be heard and the unique relationship dynamics between all parties be considered and fairly addressed.

If you would like to learn more about the Faster Payments Task Force, you can do so at its website [3]. You can find a listing of upcoming events, and recordings of previous events from the Federal Reserve here [4], and information on upcoming industry events here [5].

References

[1] https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-final-report-part1.pdf

[2] https://fedpaymentsimprovement.org/news/press-releases/faster-payments-task-force-unveils-proposals-sets-2020-target/

[3] https://fedpaymentsimprovement.org/

[4] https://fedpaymentsimprovement.org/events/fed-events/

[5] https://fedpaymentsimprovement.org/events/industry-events/

Clint Cady
Director of Payments
Nashville, TN
ccady@wcapra.com

Jim DuBoyce
Senior Consultant
Chicago, IL
jduboyce@wcapra.com

Daniel Omiliak
Consultant
Chicago, IL
domiliak@wcapra.com

Patrick Raycroft
Consultant
Chicago, IL
ptraycroft@wcapra.com

Sam Schieber
Consultant
Chicago, IL
sschieber@wcapra.com

About W. Capra

W. Capra Consulting Group is a professional services organization focused on identifying, leading, integrating and delivering technology, payment, security, and loyalty solutions to a broad range of major established retail firms and emerging businesses. We have a passion for our business and for seeing our clients succeed.

If you have additional questions regarding faster payments and its implications, please contact Clint Cady, Director of Payments.