In Pursuit of a Better Payment System

Faster Payments Task Force

Faster Payments Task Force
Criteria Discussion Document (DRAFT)

June 9, 2015

The purpose of this document is to facilitate an initial discussion of what should be included in the Task Force's criteria for assessing the effectiveness of potential faster payment approaches. The document includes: 1) background on the mission of the Task Force and purpose of the criteria, 2) several practical considerations related to applying the criteria, 3) an initial proposal for grouping together criteria into high level categories, and 4) key substantive questions for each potential criterion that might help the Task Force develop that criterion.

Background

The Faster Payments Task Force will support Strategy 2 of the Federal Reserve's Strategies for Improving the U.S. Payment System paper "to identify effective approaches for implementing safe, ubiquitous, faster payments capabilities in the United States." See Box 1 below for additional Strategy 2 details.

The Task Force's criteria for evaluating alternative faster payment approaches should be consistent with Strategy 2, as well as the broader set of "desired outcomes" set out in the Strategies Paper. These desired outcomes include –

> **Speed:** A ubiquitous, safe, faster electronic solution(s) for making a broad variety of business and personal payments, supported by a flexible and cost-effective means for payment clearing and settlement groups to settle their positions rapidly and with finality.
>
> **Security**: U.S. payment system security that remains very strong, with public confidence that remains high, and protections and incident response that keeps pace with the rapidly evolving and expanding threat environment.
>
> **Efficiency**: Greater proportion of payments originated and received electronically to reduce the average end-to-end (societal) costs of payment transactions and enable innovative payment services that deliver improved value to consumers and businesses.
>
> **International**: Better choices for U.S. consumers and businesses to send and receive convenient, cost-effective and timely cross-border payments.
>
> **Collaboration:** Needed payment system improvements are *collectively* identified and embraced by a broad array of payment participants, with material progress in implementing them.

Box 1

Federal Reserve's Strategies for Improving the U.S. Payment System, January 2015

Strategy #2 – Identify effective approach(es) for implementing a safe, ubiquitous, faster payments capability in the United States (beginning in 2015)

- Establish and lead a faster payments task force (early 2015)
- Work collaboratively with the task force and, with the input of other payment system stakeholders, assess alternative approaches for faster payments capabilities, including, for each approach, a description of the core infrastructure, security and operational changes needed for participants to interface with the infrastructure, and the estimated cost and time to implement
- Examine policy issues associated with a possible multi-provider environment, such as the framework for establishing rules (to be completed by 2016)
- Identify effective approach(es) for implementing faster payments in the United States, based on this stakeholder input and analysis (to be completed by 2016)
- Support, as appropriate, collective stakeholder efforts to implement faster payments capabilities

The remainder of this document will guide Task Force members in their efforts to define the criteria.

Practical Considerations

1. The criteria will be applied to solution proposals in conjunction with solution proposal requirements, to be established later. Criteria will generally be high level and outcome oriented whereas solution proposal requirements will ensure that certain kinds of details are documented in each proposal.
2. Solution proposals will self-identify which use cases they are targeting and Task Force members will evaluate effectiveness of a given solution in only those use cases. For example, a solution proposal that self-identifies as targeting only Person-to-Person (P2P) payments would be evaluated for effectiveness only for P2P; a solution that self-identifies as targeting P2P and business-to-business (B2B) ad hoc low value would be evaluated against both of those use cases. Ultimately, the Task Force will produce a report that compares the effectiveness of proposed solutions by use case, and the most effective solutions in one use case may differ from the most effective solutions in another.
3. Because different use cases sometimes have different needs, the assessment of whether a solution effectively meets the criteria may differ by use case. Task Force members will be given the option to differentiate their effectiveness rating of a given solution by use case.
4. Even though many of the criteria interrelate and are sometimes opposing, Task Force members should evaluate each criterion on its own merits, without consideration of these interrelationships. For example, one might believe that a criterion measuring end-user convenience is opposed to a criterion on end-user security. When evaluating the effectiveness of the solution against the convenience criterion, however, the Task Force member should consider only the convenience of that solution, regardless of whether an element of lower convenience in the solution design is tolerable because it increases security. The scoring methodology and

related weighting of each criterion will be designed to capture the balance across these interrelationships and arrive at a consolidated score that reflects the overall effectiveness of the solution.

Criteria Grouping and Key Questions

The following table suggests one possible way for the Task Force to group together sets of related criteria. Following the table, a set of key questions consequential to the development of each criterion is posed. These questions may be helpful to the Task Force as it determines the definition of each criterion, and whether additional or different criteria may be needed.

Grouping	Potential Criteria
Ubiquity	U.1 Broad Access (available to payment service providers) U.2 Broad Reach (available to and used by consumers and businesses) U.3 Applicability to multiple use cases U.4 End-user convenience U.5 Achieving "brand recognition" U.6 Consistency / predictability of end user experience U.7 Approach to Enabling Value Added Services U.8 Facilitates cross-border interoperability
Efficiency	E.1 End-users benefit from competition between solution participants E.2 Implementation Costs E.3 On-going Operating Costs E.4 Timeline for initial implementation and achieving ubiquity E.5 Compatible with modern payment format standards E.6. Comprehensive and Scalable
Safety	S.1 Credit push payment initiation S.2 Appropriate revocability, returns, denials, and exception handling S.3 Enables compliance with legal requirements, industry standards, or other practices S.4 Facilitates risk management related to settlement risk S.5 Has strong system / network security / resiliency of the operator(s)

	S.6	Requires strong system/network security/resiliency of participants
	S.7	Fosters strong end user privacy and security
	S.8	Has robust end user authentication support
Speed	F.1	Fast clearing and authorization
	F.2	Fast availability of funds to receivers
	F.3	Fast interbank settlement
	F.4	Prompt notification of payment status from end-to-end
Legal Basis	L.1	Legal framework for payments
	L.2	Licensing terms for proprietary technology
Governance	G.1	Effective, transparent and inclusive governance

Ubiquity: What key attributes are helpful in enabling ubiquity in a faster payments solution?

U.1 Broad Access (available to payment service providers)

1. Should the criteria address the ability of financial institutions or other account providers
    a. To access the solution?
        i. Is it practical for institutions of all sizes and levels of sophistication to access the solution?
    b. To ensure all of their end users can receive payments?
    c. To enable some or all of their end users to send payments?
2. Should the criteria reward –
    a. Both direct access and indirect access by financial institutions?
    b. Direct or indirect access by non-bank account providers?
    c. Low barriers to entry?
3. If a single operator solution is proposed that requires some kind of enrollment, will it achieve ubiquity? Does it have robust incentives to participate?
4. Will a multiple operator solution be able to achieve ubiquity through interoperability? If so, what additional factors or incentives need to be considered?
5. Should effectiveness of the solution in achieving broad access be measured qualitatively or quantitatively (e.g., X% of financial institutions representing Y% of end user accounts in the country can access the solution)?

U.2 Broad Reach (available to and used by consumers and businesses)

1. Should the criteria address the ability of [all? nearly all? some?] consumers and businesses to receive and/or send payments through the solution?
2. Is it desirable for a solution to –
    a. Be accessible to all end users in a use case? Most end users? Some?
    b. Provide end user access through transaction accounts, regardless of type of the account holding institution (bank vs. non-bank)?
    c. Provide consistent funds availability regardless of provider?
    d. Have incentives for financial institutions or account providers to make the solution available to all or nearly all end users for the use case(s) targeted by the solution?
    e. Motivate end-users to use the system once it is available?
    f. Address the needs of the underbanked?
    g. Provide robust, common data elements along with the payment (see U4)?

U.3 Applicability to multiple use cases

1. Should the criteria address the number and type of use cases that the solution can address?
2. Should a solution be evaluated in terms of –
    a. The initial number of targeted use cases supported?

   b. Whether the solution or its message content does not restrict use for existing or future use cases or does not require additional message types for new use cases?
   c. Whether it is generally adaptable and expandable to other use cases (targeted or otherwise) over time?

Note: Targeted use cases identified in the Federal Reserve's Strategies paper included, B2B (ad hoc low value), B2P (ad hoc high-value), B2P (ad hoc low value), P2P, P2B (ad hoc remote real time)

U.4 End-user convenience

1. Should the criteria address convenience of the solution to end-users?
2. Should this criterion reward –
   a. The variety of channels (e.g., online, remote with a mobile device, in person with a mobile device, in person without a device) the solution supports?
   b. Ability to integrate with business systems (e.g., accounts payable, accounts receivable, claims processing, payroll, treasury workstation, etc.)?
   c. Other factors?
3. Should a solution carry sufficient information to support commerce? Examples:
   a. Extended remittance information for B2B payments?
   b. Information to support biller reconciliation for bill payments?
   c. Coupon, loyalty information, location-based information, etc., to support point of sale payments?
   d. Information needed to support P2P payments?
4. Should the solution be available to end users on a 24x7x365 basis?
   a. What aspects of the payment should be available 24x7x365?

U.5 Achieving "brand recognition"

1. To what extent will it be beneficial (to achieve ubiquity) for a solution to develop a commonly used generic term (e.g., like "check", "cash", and "card") that is readily and accurately understood by users using the solution to refer to the payment method when communicating with one another?
2. How can this be measured through criteria?

U.6 Consistency / predictability of end user experience

1. Should the criteria address the consistency and predictability of the end user's experience, regardless of how the end user accesses the solution?
2. Should –
   a. A payer be able to anticipate the payee's experience in receiving the payment, for example in terms of the amount of funds received (net of fees) and the timing of receipt?
   b. The error resolution rights and liability limitations (or lack thereof) of the payer and payee be clearly defined and understood by all parties? (see also S.2)

U.7 Approach to Enabling Value Added Services

1. Should a solution –
    a. Enable participants or third party providers to build or integrate value-added services to be used by participants?
    b. Provide open or standards-based integration capabilities such as APIs, service interfaces, etc.?
    c. Utilize open standards or are proprietary standards also acceptable?
    d. Facilitate a consistent end user experience through standard communication and messaging protocols for interactions of end users with each other and with other parties (ex. account holding Institutions, 3rd Party Service Providers, etc.)?

U.8 Facilitates cross-border interoperability

1. Should the solution –
    a. Facilitate cross-border payments upon implementation?
    b. Have features that facilitate cross border payments as a subsequent phase?
        i. What features?
            1. Format features?
            2. Compliance features?
            3. Other features?

Efficiency: What key attributes enable efficiency and cost effectiveness in a faster payments solution?

E.1 End-users benefit from competition between solution participants

1. How should the solution be evaluated to ensure competition?
    a. Does it have an economic model that fosters competition by service providers on a variety of factors, including price?
    b. Does it permit new entrants as long as they meet reasonable standards that are objective and transparent?
    c. Does it enable third party providers to offer new / innovative services to solution participants as long as providers adhere to reasonable standards that are objective and transparent? (See also U.7)

E.2 Implementation Costs

1. How should the solution be evaluated in terms of the implementation costs borne by:
    a. The system operator or operators?
    b. Direct and indirect participants and third party value-added solution providers?
    c. End-users?
2. How can these costs be measured?
3. Should costs be measured in absolute terms or net of benefits?
4. If a net benefit approach is used, how would benefits be quantified?
5. Would benefits be double counted if included in this criterion, considering that other criteria reward the solution for its benefits?

E.3 On-going Operating Costs[1]

1. How should the solution be evaluated in terms of on-going operating costs borne by:
    a. The system operator or operators?
    b. Direct and indirect participants and third party value-added solution providers?
    c. End-users?
2. How can these be measured?
3. Should costs be measured in absolute terms or net of benefits?
4. If a net benefit approach is used, how would benefits be quantified?
5. Would benefits be double counted if included in this criterion, considering that other criteria reward the solution for its benefits?

[1] To be considered consistent with applicable legal principles, including laws and regulations related to antitrust or otherwise.

E.4 Timeline for initial implementation and achieving ubiquity

1. Should a solution be rewarded for a fast timeline to achieve –
   a. Initial implementation?
   b. Broad access?
   c. Broad reach and widespread use?
2. By when should these milestones be achieved?

E.5 Compatible with modern payment format standards

1. Should the solution support the ISO 20022 format?

E.6. Comprehensive and Scalable

1. Should the solution be evaluated on –
   a. The comprehensiveness of features and functions across every step of the payment process from initiation to receipt?
   b. Adequate scalability of the solution architecture to ensure that it can handle expected volumes initially and over time as the solution grows?

Safety and Security: What key attributes enable the safety and security of a faster payments solution?

S.1 Credit push payment initiation

1. Is a credit push-only model preferred? Required?
2. Are there any circumstances under which debit pulled should be allowed?
3. Will it be possible for a debit pull solution to be effective if there is a robust standardized authentication protocol? What would be the key elements of that protocol?

S.2 Appropriate revocability, returns, denials, and exception handling

1. Should the solution have clearly defined end user protections and clear rules for allocation of liability between the parties to the payment and their financial institutions for errors, exceptions, unauthorized transfers, and/or other fraud? (See also criterion U.6)
2. Should credit transfers always be final and irrevocable from the perspective of the receiver?
3. Should there be a mechanism for the payer to request voluntary return of funds from the payee for erroneous credit transfers?
4. Under what circumstances and in what ways should the solution protect consumer and/or business payers against unauthorized transfers, errors, and/or fraud?

S.3 Enables compliance with legal requirements, industry standards or other practices

The solution needs to have features (e.g., rules and technology) that make it possible for participants to comply with the legal requirements and industry standards.

1. Should we incorporate into this criterion compliance with some or all of the following?
    a. Consumer protection? (See also, criterion S.2)
    b. Cyber security (e.g., FFIEC guidelines, State regulations, NIST)?
    c. Bank Secrecy Act / Anti-Money Laundering?
    d. Sanctions Screening (e.g., OFAC)?
    e. Books and records (e.g., Record keeping requirements)?
    f. Other categories?

S.4 Facilitates risk management related to settlement risk

The solution will be expected to implement a general risk-management framework, consistent with the Part 1, Section C of the Federal Reserve's Policy on Payment System Risk (http://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf) that is appropriate for the risks the system poses to the system operator, system participants, and other relevant parties as well as the financial system more broadly.

1. Should this criterion address one or more requirements in the PSR policy for payment systems to –
    a. Identify risks clearly and set sound risk-management objectives?
    b. Establish sound governance arrangements to oversee the risk-management framework?
    c. Establish clear and appropriate rules and procedures to carry out the risk-management objectives?
    d. Employ the resources necessary to achieve the system's risk-management objectives and implement effectively its rules and procedures?
2. How should the criteria reflect other risk management controls that address settlement-related risks that arise due to –
    a. Interbank risk exposures that might result from a deferred net settlement model?
    b. Any special weekend considerations for a solution that is available to end users on a 24X7 basis?
    c. Liquidity risks that might arise between settlement cycles?
    d. Settlement in commercial bank (rather than central bank) money?

S.5 Has strong system / network security / resiliency of the operator(s)

The payment system operator(s) should have robust technical, operational, managerial, and procedural controls addressing confidentiality, integrity and availability of the solution.

1. To what extent should the solution have controls that address –
    a. Access control?
    b. Telecommunications and network security?
    c. Governance and risk management?
    d. Software development?
    e. Cryptography?
    f. Information security architecture and design?
    g. Operations security?
    h. Business continuity and disaster recovery planning?
    i. Physical (environmental) security?

S.6 Requires strong system/network security/resiliency of participants

Each participant should be required to implement technical, operational, managerial and procedural controls designed to protect the confidentiality, integrity, and availability of the IT environment, systems, and processes used by the participating institution (or its third party service provider or agent).

1. To what extent should participants be required to either establish themselves or utilize centralized services provided by the solution owner or another third party related to –
    a. Fraud detection and monitoring systems that take into account customer history and behavior and enable timely response by the institution?

b. Data security breach detection and monitoring systems that detect anomalous events?
c. Malware protection measures?
d. Controls to avoid that malicious code is exchanged through an electronic connection?
e. Procedures that handle backup media according to security practices no less secure than those applied to the participant's production systems and connectivity?
f. Disaster recovery and business continuity procedures that facilitate the timely recovery from a physical or cyber event?

S.7 Fosters strong end user privacy and security

1. Should the criteria reward solutions where –
   a. Payer and payee do not need to know each other's account numbers to initiate the payment?
   b. Payer and payee do not learn of one another's account numbers at any point throughout the lifecycle of the payment?
   c. Data is subject to layered security controls, including things like encryption in transit and/or at rest?
   d. Network rules mandate minimum security perimeter standards, internal security safeguards, and data breach detection and response standards that would apply to any organization handling sensitive data?

S.8 Has robust end user authentication support

1. Should the solution require its participants –
   a. To adopt multi-factor second level of layered end user authentication that includes at least two of the following three factors, consistent with FFIEC guidance: something you know, something you have, and/or something you are?
   b. To adopt one or more advanced security features beyond two factor authentication enhances end user authentication even further? Advanced security features may include things like three factor authentication, cryptographic key exchange, dynamic account credentials, tokenization, out of bound authentication and/or neural network intelligence to detect suspicious transactions?
   c. To define allocation of liability and develop other incentives surrounding the economic model and consumer protection regime to encourage security investments by the parties that are best positioned to control the security of each transaction?

Speed: How fast should a faster payments solution be, and in what way?

F.1 Fast clearing and authorization

F.2 Fast availability of funds to receivers

F.3 Fast interbank settlement

1. Does the need for speed of the solution vary by use case?
2. Does the following table, based on table 2 of Appendix 6 of the Strategies paper, provide appropriate minimum standards of effectiveness for each use case, and step in the payment process?
3. Should the speed criteria be further differentiated by use case? For example, should (near) real time be defined as "within seconds" for P2P payments, but "within minutes" for B2P payments?

Use cases that could benefit from faster payments	Speed of Clearing and Authorization	Availability of Funds	Speed of Settlement
P2P ***Example: Payment to friend or gardener***	(Near) Real Time	(Near) Real Time	End of Day
P2B **ad hoc remote real time** ***Example: Emergency bill pay***	(Near) Real Time	End of Day	End of Day
B2P **ad hoc low value** ***Example: Emergency payroll***	(Near) Real Time	Intra-Day	Intra-Day
B2P **ad hoc high value** ***Example: Insurance claims***	(Near) Real Time	(Near) Real Time	End of Day
B2B **ad hoc low value** ***Example: Just-in-time supplier payments***	(Near) Real Time	Intra-Day	Intra-Day

4. How should solutions that address multiple use cases be evaluated for effectiveness? Should they be held to the fastest criteria of the covered used cases? Should they be assessed independently for each covered use case?

F.4 Prompt notification of payment status from end-to-end

1. Should the solution –
    a. Facilitate prompt visibility by each party into the status of the payment at each critical juncture of the payment?
    b. Enable (or have rules mandating availability of) push notifications following some or all critical events/steps in the payment process (e.g., after authentication if a debit payment, confirmation that transaction is scheduled and good funds are on their way to an eligible recipient if a credit payment, posting of the debit to the payer, provisional posting of the credit to the payee or the debit to the payer if applicable, and final availability to the payee)?
    c. Provide mechanisms for end users to inquire on status for any critical events?

Legal Framework: How will legal issues impact the effectiveness of a faster payments solution?

L.1 Legal framework for payments

1. Given that a well-founded legal framework will be essential for any solution, how would a solution demonstrate that it has addressed –
   a. The laws and/or gaps related to the rights and obligations of all parties to the payment solution, including end users and financial institutions (and other account providers participating in the solution)?
   b. The legal basis for the activities of the system operator(s)?
   c. Set of system rules that will need to be established, if necessary?

L.2 Licensing terms for proprietary technology

Given that the Task Force Participation Agreement allows a Task Force member to "opt out" of the requirement to license to all members of the public any essential claims (as defined in the Participation Agreement) under fair, reasonable, and non-discriminatory terms, should the criteria reward, and if so, how should they reward, a solution that –

1. Incorporates essential claims where the IP owner agrees to license the solution on a fair, reasonable, and non-discriminatory basis?
2. Incorporates essential claims where the IP owner agrees to license the solution on a royalty-free basis?
3. Has no significant limitations on license use (delineate any limitations)?

Governance: What governance issues might influence the effectiveness of a faster payment solution?

G.1 Effective, transparent and inclusive governance

1. Should a solution's governance framework –
    a. Establish an effective and transparent decision making process?
    b. Take into consideration the public interest when making decisions?
    c. Have a governance body with appropriate representation from end-users and financial institutions of varying sizes, representing the solution's direct and indirect participants?
    d. Have safeguards that make it unlikely that the narrow interests of the network operator itself or any one stakeholder segment would be able to disproportionately influence outcomes to the detriment of the collective interest?
    e. Explicitly address the potential for actual, perceived, or potential conflicts of interest?
2. How might relative effectiveness of the governance model for each of these components be measured? What attributes or approaches to the governance would indicate sufficient transparency, or sufficient diversity of interests in the governance body?