In Pursuit of a Better Payment System

Faster Payments Task Force

# Faster Payments Effectiveness Criteria

January 26, 2016

# Faster Payments Effectiveness Criteria–Final Version–1-26-16

The Faster Payments Task Force was created to support Strategy 2 of the Federal Reserve's Strategies for Improving the U.S. Payment System paper to "identify effective approach(es) for implementing a safe, ubiquitous, faster payments capability in the United States." (Box 1 provides additional details on Strategy 2). This document sets out the key criteria against which each potential solution will be assessed for effectiveness by the Faster Payments Task Force.

**Desired Outcomes**

The Task Force's criteria for assessing 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

**Overview of the Effectiveness Criteria and Evaluation Scale**

Table 1 provides a high-level overview of the effectiveness criteria names, grouping them into six categories: Ubiquity, Efficiency, Safety and Security, Speed (Fast), Legal Framework, and Governance. Following table 1, summary definitions and additional considerations are documented and an effectiveness scale is established for each criterion.

**Practical and Conceptual Considerations**

This effectiveness criteria document is one of several documents being prepared by the Faster Payments Task Force to establish a process to identify effective approaches for faster payments in the United States. Other key work to be completed by the task force includes the Solution Proposal template, the assessment methodology (to guide assessment of Solution Proposals against the effectiveness criteria) and a glossary of key terms. Glossary terms are capitalized beginning with this section and hyperlinked to the glossary the first time they appear in the main body of the document, following the introduction. It will be necessary for task force members to use this criteria document in conjunction with the

other work products mentioned above. For example, one of the glossary terms, Solution, is foundational to nearly every criterion and its definition is an important complement to this document.[1]

The effectiveness criteria have been developed through a collaborative and iterative process inclusive of a diverse range of stakeholders on the Faster Payments Task Force, the Secure Payments Task Force, and the broader payments community. Two expert stakeholder work groups were established to provide recommendations on the legal and security criteria. This document represents collective views that these stakeholders have for measuring effective faster payment Solutions in the United States.

The effectiveness criteria have been designed for two main purposes. First, the criteria will be used for undertaking an assessment of Solution Proposals that are submitted to the task force for assessment. Accordingly, the criteria are comprehensive and encompass many dimensions, including some that are addressed by legacy payment Solutions and others that address gaps in legacy payment Solutions. Second, the effectiveness criteria are intended to provide guidance to the wider payments community and Payment System developers on the desired attributes of future Payment Systems according to the Faster Payments Task Force.

For Solution Proposals being submitted to the task force for assessment, it is important to note that the effectiveness criteria are not intended to be a set of minimum or maximum requirements. Instead, they are designed to provide a mechanism to differentiate the effectiveness of Solution Proposals across many dimensions. A Solution Proposal may therefore be assessed as "effective" overall, even if it falls short against a given criterion. Likewise, Solution Proposals may contain design elements or other features that exceed those described in the criteria, even if doing so does not result in a higher effectiveness rating.

Another important note is that many of the criteria interrelate and sometimes have tradeoffs. Each criterion has been developed to stand alone, without consideration of these interrelationships and/or tradeoffs. The assessment methodology to be developed by the task force will consider assessment against each criterion independently, with the balance of trade-offs captured in the overall qualitative assessment. For example, one might believe that criterion U.2 (Usability) has tradeoffs with criterion S.7 (Security controls). When evaluating a Solution against U.2, however, the assessment will consider only the usability of that Solution, regardless of whether an element of inconvenience in the Solution

[1] A Solution is the collection of Components and supporting Parties that enable the end-to-end payment process. A faster payments Solution might include new Components, the adaptation of existing Components, and/or a combination of the two. Components include any of the following: 1) rules, standards/protocols, and procedures, 2) physical or technical infrastructure, networks, systems and other resources needed by all Parties to use or enable the rules, standards/protocols and procedures, 3) centralized or shared services, if any, and 4) Legal Framework and enforcement mechanisms. Parties include any of the following: governing bodies, operators, Depository Institutions, Regulated Non-bank Account Providers, and third-party service providers.

design is tolerable because it increases security. Likewise, the assessment of the Solution against S.7 will consider only the security controls of that Solution, regardless of whether an element of lower security in the Solution design is tolerable because it increases usability.

Also, as discussed in criterion U.6 (Applicability to multiple use cases), different solution Proposals may target different use cases. The Proposal template will require Solution proposers to self-identify which use cases they are targeting and whether their Solution supports payments initiated by the Payer, the Payee, and/or a third party. The effectiveness of a given Solution will be assessed against each criterion with those use cases and payment Initiation methods in mind. For example, a Solution Proposal that self-identifies as targeting Payer-initiated person-to-person and bill payments would be assessed for effectiveness only for those use cases and payment Initiation methods.

Finally, it is noteworthy that many of the criteria require the Solution proposer to describe various elements of the Payment System Rules for the proposed Solution. In a multi-operator environment, it is possible that a single entity will be given rule-making authority by multiple operators desiring a standardized ruleset. Solution proposers planning to pursue such an approach should either coordinate with the designated rule maker or articulate preferences for rules when preparing their Solution Proposal, even though rules may not be finalized until later.

**Table 1: Criteria Groupings and Names**

| | | |
|---|---|---|
| **Ubiquity** | U.1 | Accessibility |
| | U.2 | Usability |
| | U.3 | Predictability |
| | U.4 | Contextual Data capability |
| | U.5 | Cross-border functionality |
| | U.6 | Applicability to multiple use cases |
| **Efficiency** | E.1 | Enables competition |
| | E.2 | Capability to enable value-added services |
| | E.3 | Implementation timeline |
| | E.4 | Payment format standards |
| | E.5 | Comprehensiveness |
| | E.6 | Scalability and adaptability |
| | E.7 | Exceptions and investigations process |
| **Safety and Security** | S.1 | Risk management |
| | S.2 | Payer Authorization |
| | S.3 | Payment Finality |
| | S.4 | Settlement approach |
| | S.5 | Handling disputed payments |
| | S.6 | Fraud information sharing |

| | | |
|---|---|---|
| | S.7 | Security controls |
| | S.8 | Resiliency |
| | S.9 | End-User Data protection |
| | S.10 | End-User/Provider Authentication |
| | S.11 | Participation requirements |
| **Speed (Fast)** | F.1 | Fast Approval |
| | F.2 | Fast Clearing |
| | F.3 | Fast Availability of Good Funds to Payee |
| | F.4 | Fast Settlement among Depository Institutions and Regulated Non-bank Account Providers |
| | F.5 | Prompt visibility of payment status |
| **Legal** | L.1 | Legal Framework |
| | L.2 | Payment System Rules |
| | L.3 | Consumer protections |
| | L.4 | Data privacy |
| | L.5 | Intellectual property |
| **Governance** | G.1 | Effective governance |
| | G.2 | Inclusive governance |

## Ubiquity

**U.1 Accessibility**

Accessibility means the Solution should enable any Entity (e.g., Consumer, business, government agency, or financial institution) to initiate and/or receive payments to/from any Entity consistent with applicable legal restrictions (see L.1.4).

- U.1.1 The Solution should facilitate payments to/from all types of payment Accounts based in the United States (U.S.) held at all Depository Institutions and Regulated Non-bank Account Providers[1].
- U.1.2 The Solution should demonstrate how all Entities choosing to use the Solution can be sure that their payments can reach any and all Payees.
- U.1.3 The Solution should have the ability to support Multi-currency payments.
- U.1.4 The Solution should effectively address the needs of the unbanked or underserved to affordably send or receive payments. For example, it should support the ability to make payments to/from Regulated Non-bank Provider and/or explicitly promote financial inclusion in the payments Solution.
- U.1.5 The Solution should provide a credible plan for achieving widespread adoption. The plan should demonstrate credibility by showing that the Solution is technically feasible for Providers[2] to adopt it and explaining how Providers are motivated to participate and to make the Solution available to End Users.
- U.1.6 If the Solution includes multiple operators or networks, it should have a credible plan to achieve Interoperability across these entities. The plan should demonstrate credibility by showing that a payment initiated through one operator/network/Provider can be received by a User served by another operator/network/Provider.

Very effective – The Solution fully satisfies these criteria.
Effective – The Solution mostly satisfies these criteria.
Somewhat effective – The Solution partially satisfies these criteria.

[1] Depository Institutions include those entities eligible for a Federal Reserve account. Regulated Non-bank Account Providers include money services businesses and broker-dealers subject to Federal or State regulation.

[2] The term 'Provider' is defined to include three categories of institutions/organizations: Depository institutions (any institution eligible for a Federal Reserve Account); Regulated Non-bank account providers that are classified as money services businesses, money transmitters, or broker-dealers, and are subject to Federal or State regulation; third-party service providers (e.g., non-Account holding providers of technology, software, network services, processing services, mobile wallets, equipment, security services, program managers, etc.).

| | |
|---|---|
| | Not effective – The Solution does not satisfy these criteria. |
| **U.2 Usability** | Usability means that the Solution should provide a straightforward and simple End-User experience and be available anytime, anywhere, any way, using a variety of access points.<br><br>U.2.1 The Solution should be available to End Users in a variety of circumstances, and through a variety of channels, devices, and platforms (e.g., in person without a mobile device, in person with a mobile device, remote with a mobile device, online, etc.).<br>U.2.2 The Solution should enable an Entity to initiate a payment with limited information (e.g., with a name, email address, and/or phone number) as appropriate for each use case and in a way that sufficiently supports receiver Authentication.<br>U.2.3 The Solution should be accessible to End Users on a 24x7x365 basis, including to initiate the payment, have visibility into payment status, and receive final availability of Good Funds (see F.5).<br>U.2.4 The Solution should be easy to use, accommodate varying levels of End-User technological proficiency, and address the usability needs of individuals with disabilities, the elderly, and individuals with limited English proficiency.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **U.3 Predictability** | Predictability means that the Solution should have a reliable and standard End-User experience for its baseline features.[3]<br><br>U.3.1 The Solution design should ensure that its Components and supporting Parties collectively deliver the defined baseline of core features.<br>U.3.2 Baseline features of the payment experience (timing, legal rights, costs, risks, etc.) should be defined, documented, and communicated such that they are well known by End Users and compliant with Consumer protection and commercial law (see L.1 and L.3). Aspects that might vary from one payment to the next (such as fees, timing, etc.) should be communicated by the Provider to the End User in advance and at the time of each payment. Communications should be |

[3] A Solution's baseline features are to be defined and disclosed by the Solution.

| | |
|---|---|
| | appropriate for the audience, uniform, clear, concise and easily understood so that they can be incorporated into decision making.<br>U.3.3 To facilitate a consistent experience for End Users' interaction with each other and with other Entities (e.g., Providers) the Solution should use standard communication and messaging protocols.<br>U.3.4 Baseline features should be provided consistently, regardless of the End User's choice of channel, form factor, or Provider(s) (see E.1).<br>U.3.5 The Error Resolution protections, rights, and liabilities of the Payer and Payee should be clearly defined and easily understood by all Parties as it relates to them (see S.5).<br>U.3.6 The Solution should be easily described by a commonly understood generic, brand-agnostic, term that clearly distinguishes it from other payment methods (e.g., like "check" or "cash"). Key goals of the common term are to increase adoption, confidence, and understanding of the Solution, thereby decreasing potential for confusion.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **U.4 Contextual Data capability** | Contextual Data capability means that the Solution should support the transfer or association of relevant information needed by End Users. Such information describes the reason for, or is otherwise related to the funds transfer, as appropriate to the use case.<br><br>U.4.1 Contextual Data, depending on the use case, might include, for example, biller reconciliation information, extended remittance information, Payer and Payee names and locations (as recognized by other Parties to the transaction), tax payment information, information to facilitate investigations of possible Fraud or error, loyalty/rewards information, and/or a short message to accompany payments.<br>U.4.2 The Solution should enable easy integration of contextual Data with interfacing business and personal finance systems (e.g., accounts payable, accounts receivable, claims processing, payroll, treasury workstation, Consumer accounting software, tax reporting software, etc.) where needed.<br>U.4.3 The Solution's approach to transferring or associating contextual Data should balance the need for flexibility/adaptability with the need for standards.<br><br>Very effective – The Solution fully satisfies these criteria. |

| | | |
|---|---|---|
| | | Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **U.5** | **Cross-border functionality** | Cross-border functionality means that the Solution should enable convenient, cost-effective, timely, secure and legal payments to and from other countries.<br><br>U.5.1 The Solution should provide a convenient, cost effective and timely cross-border payment method. Any special cross-border considerations for additional security measures (beyond those covered in S.1-S.11) should be addressed.<br>U.5.2 The Solution should allow for Interoperability with similar Payment Systems in other countries (see E.4 for an example of how Interoperability may be facilitated). Relevant Interoperability considerations might include differences in messaging standards, languages, character sets, mandatory Data elements, party/Account identifiers, regulatory considerations, and timing of Settlement and Good Funds availability.<br>U.5.3 The Solution should require Providers to make advance disclosure (both prior to and at the time of the Payer initiating the payment) of fees, exchange rates, and other End-User costs, as well as the timing of Good Funds availability and any risks with the payment, consistent with regulatory requirements.<br>U.5.4 The Solution should allow conversion from one currency to another as necessary for cross-border payments.<br>U.5.5 If the Solution does not have cross-border functionality at implementation, it should have a credible plan for implementing cross-border payments in the future. The plan should demonstrate credibility by showing the timeline for cross-border implementation and how the other considerations of this criterion will be addressed.<br><br>Very effective – The Solution supports inbound and outbound cross-border payments to a set of markets around the world that have Real-Time payment capabilities.<br>Effective – The Solution does not yet support cross-border payments but has a plan to do so that would fully satisfy the criteria.<br>Somewhat effective – The Solution does not yet support cross-border payments but has a plan to do so that would partially satisfy the criteria.<br>Not effective – The Solution does not satisfy the criteria. |
| **U.6** | **Applicability to** | Applicability to multiple use cases means that the Solution should support payments in multiple use cases |

| | |
|---|---|
| **multiple use cases** | (including at least one targeted use case), and should demonstrate its ability to be extensible and flexible to additional payment use cases in the future.<br><br>Note: Targeted use cases are those that were found to benefit most from faster payments capabilities by consultant research commissioned for the Federal Reserve's Strategies to Improve the U.S. Payment System paper. The use cases identified (and related examples) included: B2B - ad hoc low value (e.g., just-in-time supplier payments); B2P - ad hoc high-value (e.g., medical insurance claims); B2P - ad hoc low value (e.g., wages for temporary workers); P2P (e.g., paying a friend); P2B - ad hoc remote Real Time (e.g., emergency bill payment).<br><br>Very effective – The Solution initially supports a large number of use cases, including at least one targeted use case, and is extensible to other use cases in the future.<br>Effective – The Solution initially supports a moderate number of use cases, including at least one targeted use case, and is extensible to other use cases in the future.<br>Somewhat effective – The Solution initially supports at least one targeted use case and is extensible to other use cases in the future.<br>Not effective – The Solution does not support any of the targeted use cases. |

| Efficiency | | |
|---|---|---|
| **E.1** | **Enables competition** | Enables competition means the Solution should allow Providers to compete with each other to offer services.<br><br>E.1.1 The Solution should allow choice of Provider(s) based on factors including, but not limited to, services and price.<br>E.1.2 The Solution should allow any Entity to easily switch among Providers and/or use multiple Providers.<br>E.1.3 The Solution should require a given Provider to disclose in advance to their customer, information necessary to easily understand the total cost of using that provider.<br>E.1.4 The Solution should allow Providers, regardless of their size or incumbency, to provide services as long as the Providers meet participation requirements (see S.11).<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **E.2** | **Capability to enable value-added services** | Capability to enable value-added services means that the Solution should enable Providers to offer additional services beyond the Solution's defined baseline features.<br><br>E.2.1 The Solution should allow Providers to integrate with the Solution using open and accessible standards to offer value-added services to any Entity.<br>E.2.2 The Solution should allow Providers, regardless of their size or incumbency, to provide value-added features as long as the Providers meet participation requirements (see S.11).<br>E.2.3 The Solution should require Providers to clearly disclose to their customer that value-added services are optional.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **E.3** | **Implementation** | Implementation timeline means that the Solution should have a credible plan to achieve Initial |

| | | |
|---|---|---|
| | **timeline** | Implementation and Ubiquity (as defined in the glossary) by the target dates described in the effectiveness scale below.<br><br>E.3.1 The Solution should demonstrate a credible plan by explaining how implementation will be funded, what implementation and Ubiquity hurdles might arise, what plans exist to overcome the hurdles, which Entities expect to adopt the Solution, what market share and growth projections are used, and how the projected timelines compare to similar historical examples. The credible plan should support comprehensiveness as defined in E.5.<br><br>Very effective – Achieves Initial Implementation by 2018[4] and Ubiquity by 2020.<br>Effective – Achieves Initial Implementation by 2019 and Ubiquity by 2021.<br>Somewhat effective – Achieves Initial Implementation by 2020 and Ubiquity by 2022.<br>Not effective – Implementation timeline not credibly estimated or Initial Implementation after 2020 or achievement of Ubiquity after 2022. |
| **E.4** | **Payment format standards** | Payment format standards means that the Solution should be Interoperable with current payment format standards (e.g., ISO 20022) and adaptable to future needs and standards.<br><br>The Solution should utilize a message format that –<br><br>E.4.1 Can interface or Interoperate with existing payment format standards that are relevant to use cases targeted by the Solution (see U.4).<br>E.4.2 Enables cross-border Interoperability (see U.5).<br>E.4.3 Is cost effective to adopt.<br>E.4.4 Facilitates innovation and is adaptable for the future by permitting a mechanism for updates.<br>E.4.5 Is transparent and developed and/or published by a recognized standards development organization.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

[4] Dates refer to year end.

| | |
|---|---|
| **E.5 Comprehensiveness** | Comprehensiveness means that the Solution should support all steps of the payment process from Initiation to reconciliation.<br><br>E.5.1 The Solution should enable all relevant aspects of the end-to-end payment process, including (but possibly not limited to) – Initiation, Payer Authentication, Approval by the Payer's Provider, Clearing, receipt, Settlement, and reconciliation. To achieve this, the Solution might build new and/or interface/Interoperate with existing systems.<br>E.5.2 The technical design of the Solution should adequately support all of its features including its usability, reliability, performance, information security protocols, operations, compliance controls, and risk controls.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **E.6 Scalability and adaptability** | Scalability means the technical design of the Solution should readily support projected transaction volumes, values, and use cases. Adaptability means the technical design of the Solution should be able to readily adjust to ongoing environmental developments.<br><br>E.6.1 The technical design should support projected use cases (as determined by the Solution proposer) initially and over time.<br>E.6.2 The technical design should demonstrate the capacity to handle projected volumes and values (as determined by the Solution proposer), including increased transaction volumes and values during peak times or periods of stress and to accommodate a cushion above projections.<br>E.6.3 The technical design should be readily adaptable to ongoing developments, including those that are technological, economic (e.g., financial system failures, economic crises), regulatory, and customer demand driven.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

| | | |
|---|---|---|
| **E.7** | **Exceptions and investigations process** | Exceptions and investigations process means that the Solution should provide End Users, Providers, and any other relevant Parties with tools and protocols to minimize, identify, investigate and resolve exceptions.<br><br>E.7.1 The Solution should provide tools, including messages, alerts, notifications and related protocols, as appropriate to End Users, Providers, and any other relevant Parties, to support the ability to work together to repair or otherwise address exceptions in a reasonable time frame that is, at a minimum, compliant with applicable law and regulations (see S.5 and L.1).<br>E.7.2 The Solution should ensure that information is created, recorded, and retained for an appropriate period of time to facilitate post-transaction evaluation. For example, the Solution may facilitate case management tools with the ability to trace previously originated payments and track incidents and exceptions.<br>E.7.3 The Solution should have the ability to aggregate exceptions Data to spot patterns that may not be visible at the level of an individual Participant.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

## Safety and Security

| | |
|---|---|
| **S.1 Risk management** | Risk management means that the Solution should have a Framework (rules, policies and procedures) to address (identify, measure, monitor, and minimize) legal, credit, liquidity, operational, and other risks across the end-to-end payments process.<br><br>The Solution's risk management Framework should –<br><br>S.1.1 Address the risk of an unexpected application of a law or regulation.<br>S.1.2 Address risks related to the Solution's Settlement approach (see S.4).<br>S.1.3 Address operational risks related to deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events (see S.8).<br>S.1.4 Address the risk of unauthorized, Fraudulent (including first-, second- and third-party fraud, and fraud in the inducement), or erroneous payments (see S.3, S.5, S.7, and S.10).<br>S.1.5 Include incentives (i.e., positive, negative, financial, or non-financial) to operators and Providers to address and contain risks they pose to other Participants.<br>S.1.6 Be subjected to periodic review and update.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.2 Payer Authorization** | Payer Authorization, including pre-authorization, means that the Solution should require payments to be initiated only with the explicit and informed consent (see U.3.2) of the Payer to the Payer's Depository Institution or Regulated Non-bank Account Provider.<br><br>S.2.1 The Solution should require the Payer to Authorize to their Depository Institution/Regulated Non-bank Account Provider concurrently with payment Initiation each payment, unless the payment is pre-authorized prior to payment Initiation.<br>S.2.2 If the Solution allows pre-authorization, it should enable the Payer to pre-authorize the Payer's Depository Institution or Regulated Non-bank Account Provider to make one or more payments based on defined parameters, as relevant to those payments (e.g., Account from which funds are drawn, Payee, frequency, time and date, amount, amount limits, duration of Authorization, etc.) The set of pre-authorizations made by the Payer should subsequently be |

| | |
|---|---|
| | visible to the Payer.<br>S.2.3 If the Solution allows pre-authorization, it should enable the Payer to revoke any pre-authorization of payments easily and timely, or to change relevant pre-authorization parameters easily and timely.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.3 Payment Finality** | Payment Finality means that the Solution should define a point in time after which a payment is Irrevocable. (See S.5 regarding protections to Payers for Fraudulent or erroneous payments).<br><br>S.3.1 The Solution should require the Payer's Depository Institution or Regulated Non-bank Account Provider to approve each payment following payment Initiation to assure the Payer's Account has Good Funds.<br><br>Note: In assuring Good Funds, the Solution should foster Consumer control and understanding of Account management implications and any related fees; the permissibility of overdrafts should be decided by an appropriate regulatory authority and the Solution should demonstrate compliance with all regulatory guidance related to overdrafts and credit, as applicable.<br><br>S.3.2 The Solution should architecturally enable, and have rules and/or a supporting Legal Framework that clarifies exactly when the payment becomes Irrevocable, but this should be after Good Funds Approval and no later than when funds are made available to the Payee. The exact point of Irrevocability should be easily understood by and visible to the Payee (see F.5).<br>S.3.3 The Solution should provide mechanisms and processes to protect or compensate the Payer in the event that the payment is disputed and to comply with relevant Consumer protection regulations, including Regulation E (see S.5 and L.1).<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

| | |
|---|---|
| **S.4 Settlement approach** | Settlement approach means the Solution should, by its design and rules, determine when and how Depository Institutions and Regulated Non-bank Account Providers settle their obligations between each other; it should also determine the mechanisms to pro-actively manage any related credit and liquidity risks.<br><br>S.4.1 The Solution's rules should define when and how Depository Institutions and Regulated Non-bank Account Providers settle obligations to one another arising from End User payments (e.g., Real-Time gross Settlement, deferred net Settlement, frequency of Settlement, hours of Settlement operation, etc.). The Solution's participation requirements should be designed to ensure that compliant Depository Institutions and Regulated Non-bank Account Providers have the operational, financial, and legal capacity to fulfill their obligations, including to other Providers, on a timely basis. Where a Depository Institution or Regulated Non-bank Account Provider settles on behalf of others, it may be appropriate for the Solution to impose additional requirements to ensure that the settler has the financial and operational capacity to do so.<br>S.4.2 The Solution's risk management Framework should have an approach to pro-actively manage inter-Provider credit and liquidity risk exposures arising from any lag between transaction Finality and inter-Provider Settlement and to ensure that credit exposures to each Provider can be fully covered. Any special credit and liquidity risk considerations for a Solution that is available to End Users on a 24x7x365 basis should be addressed.<br>S.4.3 The Solution should either enable Settlement in central bank money, or minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money for the inter-Provider Settlement process.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.5 Handling disputed payments** | Handling disputed payments means that the Solution should have rules, processes and timeframes for effectively addressing unauthorized, Fraudulent, erroneous, or otherwise disputed payments, and, for each of these, have an appropriate allocation of liability among, and substantive liability limits for, all |

| | |
|---|---|
| | Parties, including the Payer, the Payee, and the Providers involved in the payment. (See S.3 regarding payment Finality).<br><br>S.5.1 The Solution's rules should include requirements, processes and timeframes for addressing unauthorized, Fraudulent, erroneous, or otherwise disputed payments, as well as mechanisms to hold rule violators accountable. For example, the Solution should include mechanisms to block funds availability (in a way that is consistent with any applicable laws and/or regulations) if an unauthorized, Fraudulent, or erroneous payment is reasonably identified by the receiving Depository Institution or Regulated Non-bank Account Provider prior to payment Finality.<br>S.5.2 The Solution should make clear how a Consumer Payer's Provider can comply with Consumer protection laws related to Error Resolution and Fraudulent or unauthorized payments; this does not apply to first-party fraud, which is covered in S.1.4.<br>S.5.3 The Solution should provide mechanisms for any party to the transaction to request prompt voluntary return of funds from the Payee, or the return of funds as required by law.<br>S.5.4 The Solution should adopt an approach, including the delineation of roles, responsibilities and liability allocation, which reasonably protects business and government Payers against losses related to Fraud or errors and adheres to applicable laws or regulations.<br>S.5.5 The Solution should adopt an approach, including the delineation of roles, responsibilities and liability allocation, which reasonably protects Consumer Payers against losses related to Fraud or errors and adheres to applicable laws or regulations (e.g., Regulation E and Regulation Z).<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.6 Fraud information sharing** | Fraud information sharing means that the Solution should require and facilitate timely and frequent sharing of information among all Providers, operators and regulators to help them manage, monitor, and mitigate Fraud and evolving threats in accordance with applicable law (see L.4).<br><br>S.6.1 The Solution should require the sharing of information to facilitate managing and monitoring Fraud (e.g., patterns suggestive of risk, known instances of Fraud, known vulnerabilities, the significance of the information and effective mitigation techniques). Information shared for anti-fraud activities should be used only for fraud management purposes. Whenever possible, personally identifiable information should be excluded from information sharing. If shared, |

| | |
|---|---|
| | such information should be encrypted (see S.9 and L.4).<br>S.6.2 The Solution should describe how Data owned by Entities other than Providers and operators would be aggregated, managed and protected for purposes of Fraud information sharing.<br>S.6.3 The Solution should facilitate information sharing that supports Real-Time and ex-post management and monitoring of Fraud, and provides timely updates and alerts.<br>S.6.4 The Solution's information sharing mechanisms should be easy to implement, update and maintain.<br>S.6.5 The Solution's information sharing mechanisms should support differential access to content based on the roles and responsibilities of each operator, Provider and regulator.<br>S.6.6 The Solution's information sharing mechanisms may include a central authoritative trusted repository to perform functions such as storage and aggregation of the information.<br>S.6.7 The Solution should have the ability to aggregate Fraud information to spot patterns that may not be visible at the level of an individual Participant.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.7 Security controls** | Security controls means that the Solution has layered and robust technical, access, operational, procedural, and managerial controls to address and foster security, including but not limited to the integrity and protection of confidential, private and sensitive Data.<br><br>S.7.1 The Solution should provide strong technical access components and controls, including –<br>• Identity verification and access management<br>• Data encryption in-transit and at-rest<br>• Data quality and integrity controls<br>• Data breach prevention and detection<br>• Layered security controls (e.g., The Open Systems Interconnect, OSI)<br>• Components and controls that leverage and are consistent with industry standards (e.g., NIST, ISO, ANSI).<br>S.7.2 The Solution should provide strong operational and procedural components and controls, including –<br>• Data retention and disposal controls |

| | |
|---|---|
| | • Physical (environmental) security<br>• Operations security, monitoring, and incident response<br>• Communications and network security.<br>S.7.3 The Solution should have strong managerial policies and oversight that –<br>• Integrate with existing risk management processes<br>• Are adaptable to enterprise-level security architectures<br>• Comply with Provider-specific governance and risk management attributes (see S.1).<br>• Motivate investments by all Parties to collectively and continuously improve the security of each transaction.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.8 Resiliency** | Resiliency means that the Solution has mechanisms and systems to ensure high levels of end-to-end availability and reliability under normal and stressed operating conditions.<br><br>S.8.1 The Solution should define its target availability metrics and describe its approach to ensure those metrics can be achieved.<br>S.8.2 The Solution should have business continuity and disaster recovery plans to ensure timely recovery and resumption of critical services in the event of an outage or a cyber-attack.<br>S.8.3 The Solution should have mechanisms to minimize the chance that an adverse Solution-related event will cause other market participants to fail to meet their obligations (i.e., trigger systemic risk).<br>S.8.4 The Solution should demonstrate that sufficient resources are devoted to business continuity and resiliency.<br>S.8.5 The Solution should conduct regular contingency testing across all operators and providers of its end-to-end systems.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

| | |
|---|---|
| **S.9 End-User Data protection** | End-User Data protection means that the Solution should have controls and mechanisms to prevent the unintended exposure of End-User Data. End-User Data, both digital and physical, should be protected in transit and at rest, before, during, and after a transaction, so that it is not exposed in-the-clear.<br><br>S.9.1 The Solution should require that all operators and Providers through the end-to-end payments process have robust controls and mechanisms (including for End Users), appropriate to their roles, to protect sensitive information (see also L.4).<br>S.9.2 The Solution should have controls and mechanisms to protect sensitive information needed for Account setup, transaction setup and problem resolution from unnecessary disclosure. For example, the Payer and Payee should not need to know each other's Account numbers or other sensitive information to initiate or receive the payment.<br>S.9.3 The Solution should have controls and mechanisms to protect any sensitive information that is needed to process and complete a payment. For example, the Payer and Payee should not learn of one another's Account numbers or other sensitive information at any point throughout the end-to-end payment process.<br><br>Note: Sensitive information should be defined by the Solution consistent with applicable Federal and/or State law.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.10 End-User/Provider Authentication** | End-User/Provider Authentication means the Solution should require robust identification and verification for enrolling and transacting with End Users and Providers.<br><br>S.10.1 The Solution should define a robust Framework that operators and Providers will use to Authenticate Providers and End Users to the system.<br>S.10.2 The Solution should have robust mechanisms to ensure the payment is destined to reach the intended Payee at the intended Payee Account. For example, the Solution might (a) require the Payee's Provider to explicitly communicate Acceptance of a payment before finalizing the transaction, (b) provide a mechanism for sending a pre-notification or "test message" to help confirm the identity of the Payee and to validate the existence of the Payee's Account, and/or |

| | |
|---|---|
| | (c) require monitoring for payment anomalies (see S.7.2).<br>S.10.3 The Solution should align with regulatory guidance (e.g., FFIEC) and industry standards (e.g., ANSI, ISO, W3C, etc.) for End-User Authentication.<br>S.10.4 The Solution should apply strong End-User Authentication controls across all delivery channels and may vary the Authentication procedure based on the risk-weighting of a given transaction.<br>S.10.5 The Solution should enable the End User to be Authenticated initially to the Solution itself (at enrollment and prior to multiple transactions), and should also require Providers to re-Authenticate End Users based on the risk-weighting of a transaction.<br>S.10.6 The Solution should be able to adopt new and decommission old Authentication models based on the evolving threat landscape.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **S.11 Participation requirements** | Participation requirements means that the Solution should establish and monitor compliance with transparent requisites that Providers must adhere to on an ongoing basis as appropriate to their roles in the Solution.<br><br>S.11.1 The Solution's participation requirements should be adequate to ensure that all Providers adhere to the Solution's rules and requirements relevant to their role, including those related to security, resiliency, anti-money laundering/know your customer, and Data privacy/integrity protocols. See also criteria S.5-S.10.<br>S.11.2 The Solution's participation requirements should be adequate to ensure that all compliant Depository Institutions and Regulated Non-bank Account Providers have the operational, financial, and legal capacity to fulfill their obligations, including to other Providers, on a timely basis (see S.4).<br>S.11.3 The Solution should have processes to monitor and ensure compliance by all Providers against these requirements.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

| Speed (Fast) | | |
|---|---|---|
| **F.1** | **Fast Approval** | Fast Approval means that the Solution should require and enable the Payer's Depository Institution or Regulated Non-bank Account Provider to assure Good Funds for each payment in a timely manner, as indicated by the effectiveness scale below.<br><br>Note: This criterion is measured from the completion of payment Initiation (just following Payer Authorization to their Provider, or just following confirmation by the Payer's Provider that pre-authorization exists for a given payment) to the point when the Payer's Depository Institution or Regulated Non-bank Account Provider approves or denies the payment.<br><br>Very effective – Within 2 seconds.<br>Effective – Within 5 seconds.<br>Somewhat effective – Within 15 seconds.<br>Not effective – Over 15 seconds. |
| **F.2** | **Fast Clearing** | Fast Clearing means that the Solution should require and enable the Payer's and Payee's Depository Institution or Regulated Non-bank Account Provider to exchange payment information in a timely manner, as indicated by the effectiveness scale below.<br><br>Note: This criterion is measured from the completion of payment Initiation (just following Payer Authorization to their Provider, or just following confirmation by the Payer's Provider that pre-authorization exists for a given payment) to the point when payment information is exchanged among the Payer's and Payee's Depository Institution or Regulated Non-bank Account Provider.<br><br>Very effective – Within 2 seconds.<br>Effective – Within 5 seconds.<br>Somewhat effective – Within 1 minute.<br>Not effective – Over 1 minute. |
| **F.3** | **Fast availability of Good Funds to the Payee** | Fast availability of Good Funds to the Payee means that the Solution should require and enable funds and contextual Data, as appropriate (see U.4), to be received by the Payee, such that the funds can be withdrawn or transferred in a timely manner, as indicated by the effectiveness scale below. |

| | | |
|---|---|---|
| | | Note: This criterion is measured from the completion of payment Initiation (just following Payer Authorization to their Provider, or just following confirmation by the Payer's Provider that pre-authorization exists for a given payment) to the point when funds can be withdrawn or transferred by the Payee.<br><br>Very effective – Within 1 minute.<br>Effective – Within 30 minutes.<br>Somewhat effective – Within 1 hour.<br>Not effective – Over 1 hour. |
| **F.4** | **Fast Settlement among Depository Institutions and Regulated Non-bank Account Providers** | Fast Settlement means that the Solution should require and enable obligations between the Payer's and Payee's Depository Institution or Regulated Non-bank Account Provider to be discharged in a timely manner, as indicated by the effectiveness scale below.<br><br>F.4.1 The Solution should have an approach to manage credit and liquidity risk exposures arising from any lag between transaction Finality to the Payee and inter-Provider Settlement, including for example if a Solution is available to end users on a 24x7x365 basis but inter-Provider Settlement is not (see S.4).<br>F.4.2 Any special considerations for handling Settlement between Depository Institutions or Regulated Non-bank Account Providers located in different time zones should be addressed.<br>F.4.3 The Solution may provide flexibility to the Depository Institution or Regulated Non-bank Account Provider to determine the timing of Settlement (e.g. the Depository Institution or Regulated Non-bank Account Provider might choose immediate or deferred Settlement) as long as the associated risks of deferred Settlement are managed (see F.4.1).<br><br>Note: This criterion is measured from the completion of payment Initiation (just following Payer Authorization to their Provider, or just following confirmation by the Payer's Provider that pre-authorization exists for a given payment) to the point of Settlement.<br><br>Very effective – Less than 30 minutes and otherwise fully satisfies these criteria.<br>Effective – Less than 2 hours and otherwise mostly or fully satisfies these criteria.<br>Somewhat effective – No later than end of day and otherwise partially, mostly, or fully satisfies these criteria.<br>Not effective – Next day or longer, or does not otherwise satisfy these criteria. |
| **F.5** | **Prompt visibility of** | Prompt visibility of payment status means that the Solution should enable mechanisms by which both the |

| | |
|---|---|
| **payment status** | Payer and the Payee can track the payment at various stages of the end-to-end payment process in a timely manner, as indicated by the effectiveness scale below.<br><br>F.5.1 For the Payer, this should include visibility of when their payment has been approved (see F.1), their Account has been debited, and the Payee has received the funds in their Account for use.<br>F.5.2 For the Payee, this should include visibility of when the payment has been approved (see F.1) and when funds become available for use in their Account.<br><br>Note: This criterion is measured from the time a given step/status is achieved to when that status is visible to the relevant Parties. For example, if it takes 30 minutes following the completion of payment Initiation for Good Funds to become available to the Payee, but this change in status is made visible to Parties 5 seconds after availability, the Solution would be rated very effective for this criterion if visibility of status is provided 30 minutes and 5 seconds after Initiation. Visibility can be achieved, for example, either via push (notification) or pull (response to a query).<br><br>Very effective – Within 5 seconds.<br>Effective – Within 15 seconds.<br>Somewhat effective – Within 1 minute.<br>Not effective – Over 1 minute. |

# Legal Framework

| | |
|---|---|
| **L.1 Legal Framework** | Legal Framework means that the Solution should describe the legal sources which will govern the operation of the Solution and/or impose any compliance obligations on the Solution or End Users, and describe any contemplated changes or additions to existing laws necessary to support the Solution.<br><br>L.1.1 The Solution should identify relevant and applicable legal sources such as existing public sector laws, regulations, regulatory interpretations or rulings, court decisions and/or Payment System Rules that will apply to the Payment System, End Users, Providers, Payers and Payees, and payments through the Payment System.<br>L.1.2 The Solution should identify any known gaps in legal sources with respect to the proposed Legal Framework for the Solution and describe any plans to address those gaps.<br>L.1.3 The Solution should describe how Entities and payments through the Payment System (from Payer to Payee) will be legally bound within the proposed Legal Framework for the Solution.<br>L.1.4 The Solution should describe how it supports compliance with relevant U.S. law by all End Users and Providers when sending and receiving payments. U.S. law includes OFAC, AML, BSA, the UIGEA (Regulation GG), Federal Consumer protection regulations (such as Regulation E and Regulation Z), Federal and State MSB laws, and all other applicable Federal and State laws.<br>L.1.5 The Solution should identify any unique legal provisions needed in the Solution's Legal Framework to address any situations in which End Users/Providers will perform the same functions in the Payment System, but are subject to different applicable U.S. banking and payment laws and/or regulatory supervision.<br><br>Very effective – The Solution fully satisfies these criteria. Note: the Solution can meet the very effective standard even if the Legal Framework is based on the assumption that Payment System Rules will be used to supplement existing payment law or regulations (see L.2 below.)<br>Effective – The Solution mostly satisfies these criteria (e.g., is dependent on minimal changes to Federal regulations to implement the Legal Framework)<br>Somewhat effective – The Solution partially satisfies these criteria (e.g., is dependent on minimal changes to Federal regulations and Federal/State statutes to implement the Legal Framework).<br>Not effective – The Solution does not satisfy these criteria. |

| | |
|---|---|
| **L.2 Payment System Rules** | Payment System Rules means that the Solution should have requirements, standards/protocols and procedures that govern the rights and obligations of all End Users, Providers, Payers and Payees.<br><br>L.2.1 The Solution should describe key features of existing or proposed Payment System Rules governing the rights and obligations of all End Users, Providers, Payers and Payees to enable the Payment System to operate effectively and efficiently, including Payment System Rules addressing:<br>L.2.1.1 Authentication of all Entities, payments or messages connected to a payment;<br>L.2.1.2 Legal responsibility of Providers that provide Payment System access to End Users;<br>L.2.1.3 Payment Order Initiation/Authorization and termination of Authorization;<br>L.2.1.4 Cancellation of a Payment;<br>L.2.1.5 Delayed and failed payments;<br>L.2.1.6 Payment Finality and Settlement;<br>L.2.1.7 Timing of sending and receipt of a payment;<br>L.2.1.8 Records as proof of payment for Payers and Payees; and<br>L.2.1.9 Error Resolution for anticipated disputed payments (see S.5) among End Users, Providers, Payers and Payees.<br>L.2.2 If different than the process set forth in G.1 and G.2, the Solution should describe the process that was or will be used for the development and amendment of the Payment System Rules, including the process for obtaining input from Payment System stakeholders.<br>L.2.3 If different than the process set forth in G.1 and G.2, the Solution should describe how Payment System Rules will be enforced and monitored, including whether or not an organization or regulators may enforce the rules.<br>L.2.4 The Solution should describe existing or proposed Payment System Rules for allocating legal responsibility to appropriate Entities to obtain valid Authorization from the Payer.<br>L.2.5 The Solution should describe existing or proposed Payment System Rules related to an Error Resolution process within the Payment System for End Users and Providers to correct or otherwise resolve errors, unauthorized transactions or disputes in the payment process (see also S.5 and L.3).<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

| | |
|---|---|
| **L.3 Consumer protections** | Consumer protections means that the Solution should have a Legal Framework and procedures that allocate legal responsibility, allocate financial responsibility and support Error Resolution for payments made to or from natural persons for personal, family, or household purposes (see also S.5).<br><br>L.3.1 The Solution should describe a Legal Framework for allocating legal and financial responsibility for all Entities for losses in the event of a Payer or Payee claim of unauthorized, Fraudulent or erroneous Consumer payments.<br>L.3.2 The Solution should establish Payment System Rules and procedures that support Error Resolution for Consumer claims arising from payments Fraud, unauthorized payments or errors.<br>L.3.3 The Solution should include option(s) for End Users, Providers and/or the Payment System to establish additional Consumer protections for payments, which may exceed those protections that are otherwise required under applicable law.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **L.4 Data privacy** | Data privacy means that the Solution should have an approach to identify whether and how payment and related information can be collected and disclosed, consistent with applicable policy, law, and End-User preference. The Solution should also have an approach, consistent with law, to secure information that should not be disclosed (see also S.6 and S.9).<br><br>L.4.1 The Solution should describe its approach to Data privacy and Confidentiality of payment and related Data. For example, the Legal Framework should describe limitations on End Users' or Providers' collection of Data and use or disclosure of payment Data to third Parties.<br>L.4.2 The Solution should describe its approach to Data security of payment and related Data, taking into consideration the application of legal requirements. For example, the Legal Framework should describe operational procedures and policies to secure Data within the Payment System and at End-User and Provider locations.<br>L.4.3 The Solution should describe the nature and type of End-User Data that may be required for security, legal compliance and Authentication purposes within the Solution.<br>L.4.4 The Solution should describe how End Users may get visibility into the Data being collected on them, limit sharing of such Data, and change their privacy preferences with regard to proposed uses of End-User Data. |

| | |
|---|---|
| | L.4.5 The Solution should describe its approach to Data breaches at the Payment System or at an End User/Provider, the responsibilities (including notifications) of the End Users/Providers in the event of such a breach, and whether the Legal Framework seeks to allocate financial or other responsibility among End Users and Providers in the event of a Data breach.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **L.5 Intellectual property** | Intellectual property means that the Solution should have an approach to address any risks arising from third-party rights related to patents, trademarks, copyrights, and trade secrets.<br><br>L.5.1 The Solution should set forth a proposed approach for the Payment System, End Users and Providers to resolve or manage, prior to implementation, any legal, operational or financial risks arising from third-party intellectual property rights (including patents, trademarks, copyrights and trade secrets). This proposed approach should include whether or not the Solution has undertaken or will undertake a due diligence review of potentially applicable intellectual property rights.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |

| Governance | |
|---|---|
| **G.1 Effective governance** | Effective governance means that the Solution should have decision and rule-making processes that are transparent and support both the Solution's objectives and Public Policy Objectives.<br><br>G.1.1 The Solution's governance arrangements (e.g., policies and structure) should ensure efficient decision making and rule making, including establishing clear lines of responsibility for all decision makers or decision-making bodies.<br>G.1.2 The Solution's governance arrangements should be publicly disclosed.<br>G.1.3 The Solution's governance arrangements should provide a process to handle appeals related to specific decisions or their implementation.<br>G.1.4 The Solution's governance arrangements should provide for independent validation of compliance with the Solution's rules, compliance with applicable law, and achievement of both the Solution's objectives and public policy objectives.<br><br>Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |
| **G.2 Inclusive governance** | Inclusive governance means the Solution should allow for input and representation from diverse stakeholders (e.g., End Users, operators, Providers, and regulators), and supports the public interest.<br><br>G.2.1 The Solution's governance arrangements should include consideration of the public interest when making decisions and rules.<br>G.2.2 The Solution's governance arrangements should provide for input and influence by all stakeholders, through one or more governance or advisory bodies.<br>G.2.3 The Solution should have governance and advisory bodies that fairly represent stakeholders' interests and risks.<br>G.2.4 The Solution's governance approach should enable specific stakeholders or stakeholder groups to proportionately influence outcomes.<br>G.2.5 The Solution's governance approach should address and manage actual, perceived, or potential conflicts of interest. |

| | |
|---|---|
| | Very effective – The Solution fully satisfies these criteria.<br>Effective – The Solution mostly satisfies these criteria.<br>Somewhat effective – The Solution partially satisfies these criteria.<br>Not effective – The Solution does not satisfy these criteria. |