

In Pursuit of a Better Payment System

Secure Payments Task Force



Federal Reserve System Secure Payments Task Force Teleconference September 16, 2015

Agenda

Topics/Speakers	Welcome and Agenda Review	Gordon Werkema
	Recap of August 25-26 Meeting Hopes, Fears, Success Statements	Barb Pacheco
	Faster Payments Security Criteria	Kylie Stewart
	Areas of Focus and Priorities for Action Advising the Fed	Barb Pacheco
	Engagement Planning Identifying Task Force Education Needs	Connie Theien
	Upcoming Meetings and Key Deliverables	Todd Aadland

Anti-Trust Compliance Statement

Task Force Participants are expected to ensure that their participation and communications at Task Force meetings do not violate antitrust laws.

This means that no activity or discussion at our meetings or other related functions may be engaged in for the purpose of bringing about any understanding or agreement among participants to do any of the following: (a) raise, stabilize, or set future prices; (b) regulate future production levels among individual participants; (c) allocate geographic markets or customers; (d) encourage boycotts or seek to exclude specific participants; or (e) aid in creating improper monopolies.

In addition, participants should avoid discussing or revealing any individual participant's competitively sensitive information, including any participant's prices, discounts, costs, capacity, inventory, sales, future business plans, or bids for contracts.

Any questions regarding the meaning or applicability of this statement, as well as any concerns regarding activities or discussions at Task Force meetings, should be promptly brought to the attention of counsel for the Federal Reserve Bank, present at the meeting.



Recap of August 25-26 Task Force Meeting and Hopes, Fears, Success Statements

Barb Pacheco

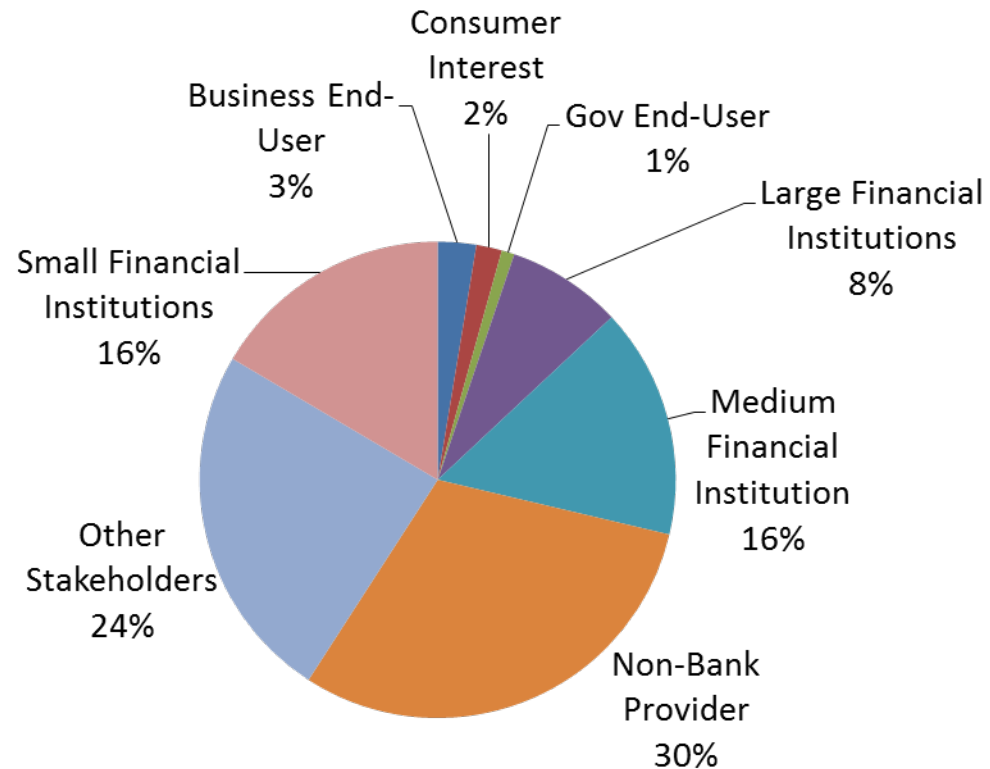
FEDERAL RESERVE BANK OF NEW YORK FINANCIAL SERVICES

Secure Payments Task Force

Kick Off Meeting (August 25–26)

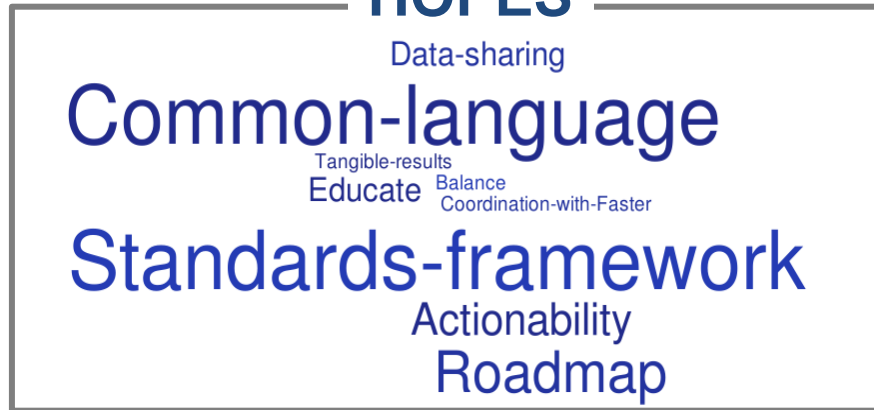
Registered members of the Secure Payments Task Force: **175**

Members who attended the Aug 25-26 in-person meeting: **112**



Hopes, Fears and Success Statements

HOPES



FEARS



Success Statements

The following success statements received the top votes from the Task Force

1. A framework that does not stifle **innovation** and new payment technology, yet achieves a **measurable reduction in fraud**
2. Solutions are **flexible and adapt** to ever-changing threats, technology capabilities and players in the payment system
3. There is a **common lexicon** that is used to tackle and measure payment security issues
4. A plan for **workable solutions** that is **tangible**, with **broad support**, that ensures **all stakeholders** are informed and educated.
5. **Balance** the benefits of the **various** payment ecosystem participants

Choose from one of the following choices using the webinar tool:

- A. I would endorse these success statements as they are written
- B. I would endorse these success statements with minor changes
- C. I would not endorse these success statements without substantive changes

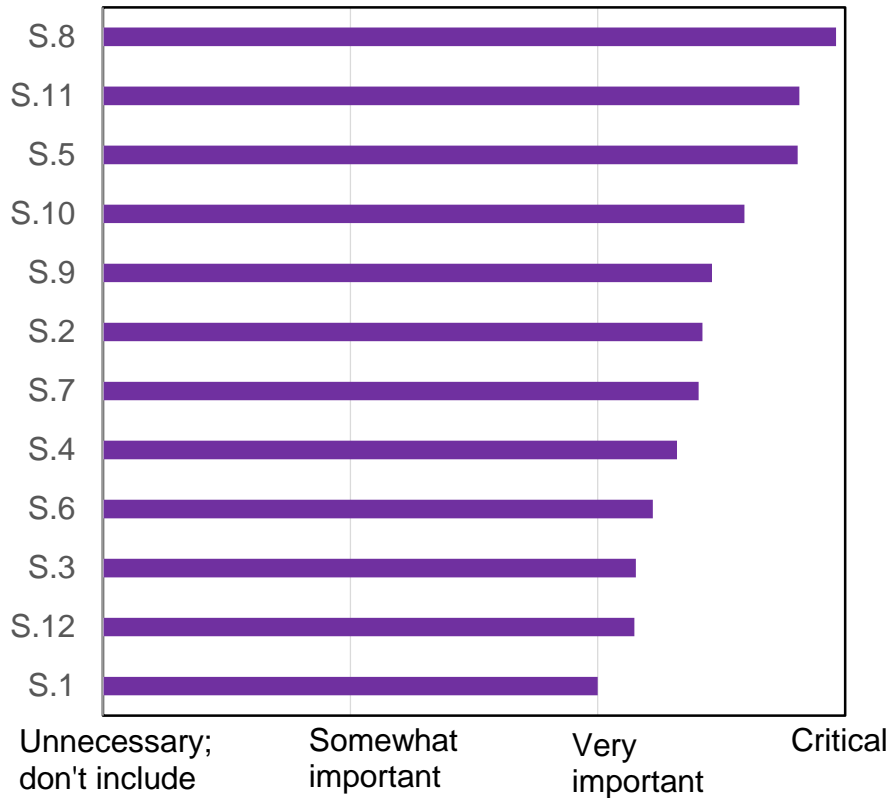


Security Criteria: Survey Results, Task Force Discussion, and Special Work Group

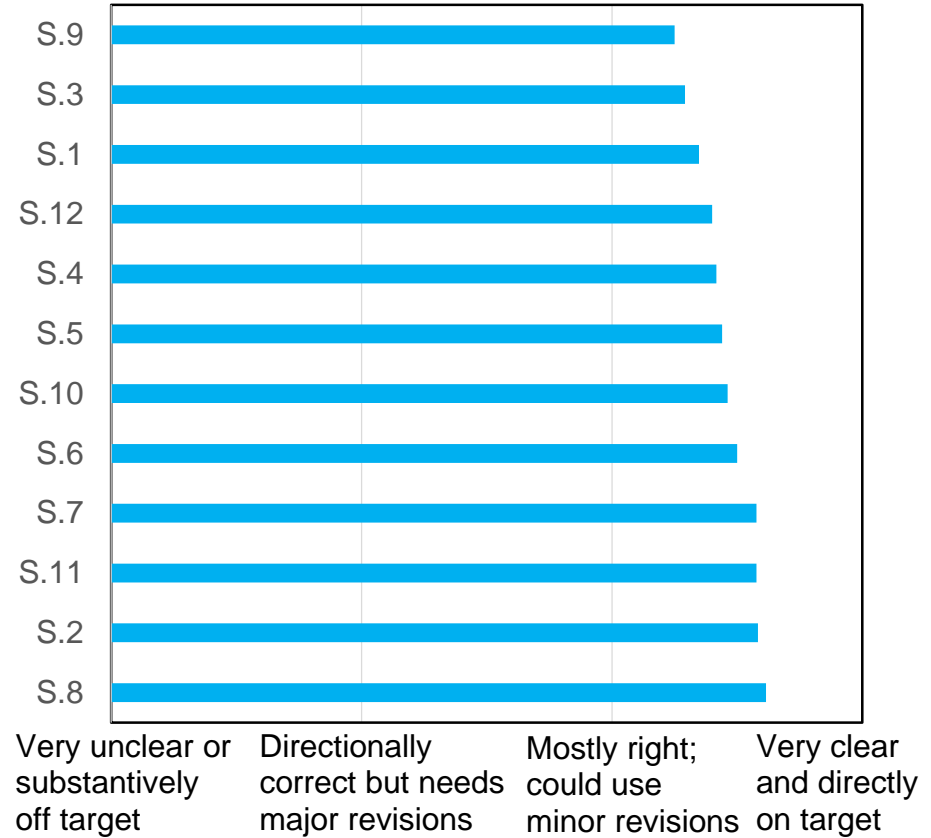
Kylie Stewart and Barb Pacheco

Secure Payments Task Force Survey Results

Importance



Clear and Appropriate



Number of Responses = 28

Selected Issues from Task Force Discussion

S.1 Payment initiation

- Should be less about credit push and debit pull, and more about security

S.2 Authorization

- Authorization should be about the payer (the definition includes authorization by both the payer and their provider)

S.3 Finality and irrevocability

- System should support resolution of disputes, errors and fraud
- Requirement is reasonable for domestic transactions, but more difficult for cross-border

S.4 Settlement

- Should compare to existing settlement capabilities

Selected Issues from Task Force Discussion

S.5 Fraudulent or erroneous payments

- Separate criterion for fraudulent and erroneous transactions
- Should indicate how it prevents errors and fraudulent transactions

S.6 Fraud information sharing

- Considerations for: new legal requirements, and emerging standards and technologies; voluntary sharing; central authoritative trusted repository; standardized data formats; and priority of information

S.7 Enables robust compliance with law

- Combine with other compliance and standards in one criterion
- Consider AML/BSA/OFAC and whether it covers all state laws

S.8 Security controls

- Needs more granular breakdown and quantifiable metrics
- Include additional frameworks – ISO, ANSI, NIST, PCI, DSS

Selected Issues from Task Force Discussion

S.9 Strong resiliency

- New consideration S.9.3 – systemic fail-safes required
- Separate business continuity and disaster recovery

S.10 End user privacy

- Data elements that must be protected: Social Security Number, signature, biometric self-selected information e.g., PIN, challenge questions, account number.

S.11 End user authentication

- Simplified criterion to risk-based layered authentication
- Criterion drafting appeared old (based on current standards)

S.12 Risk based participation requirements

- Needs to include the supply chain
- Need to consider who will maintain a trusted provider list

Security Criteria Work Group

Focus on:

- S.5: Fraudulent or erroneous payments
- S.8: Security controls
- S.10: End user privacy
- S.11: End user authentication

Would benefit most from further expert feedback

Are among most important security criteria according to both Faster and Secure Payments Task Force surveys

Generated substantial discussion at Task Force meeting

Other security criteria work in process:

- S.1-S.3: under revision from Faster Payments Task Force feedback



Areas of Focus and Priorities for Action

Barb Pacheco

Areas of Focus and Potential Work Groups

August 26 Breakout Draft Session Summary

Area of Focus: A – Payment Identity Management and Authentication

Work Group Topic		Work Group Objective
A-1	Hooking into overarching industry / sector efforts	Identification, collaboration and execution of existing industry efforts (e.g., hardware, software, payment groups)
A-2	Enrollment model consistency	Create an enrollment process that secures the payment process that identifies the user on a risk adjusted basis. The process will also be extensible to other industry needs, respect privacy, minimize the need for PII, and creates a zone of privacy.
A-3	End point experience (speed)	Develop a set of common controls and attributes for end point authentication

Area of Focus: B – Fraud and Risk Technologies, Solutions and Best Practices

Work Group Topic		Work Group Objective
B-1	Anomaly Detection and Analytics	Identify tools, data sets, reporting services and best practices that facilitate analytics to detect and/or prevent anomalies
B-2	Vulnerability management	Establish standardized protocols for identifying, assessing and remediating vulnerabilities throughout the payment chain
B-3	Data protection	Define what data to protect, when (in process and stored) and how

Areas of Focus and Potential Work Groups

August 26 Breakout Draft Session Summary

Area of Focus: C – Fraud / Cyber Information Sharing and Privacy Protections

Work Group Topic		Work Group Objective
C-1	Misaligned laws and regulations and motivations to share information	Evaluate legal, legislative, regulatory and joint industry environment as it applies to current / evolving payment systems and make recommendations, as needed
C-2	What information is shared, who is it shared with, how is it shared and what are the rules for the use of the data (who, what, when, where, why – sharing)?	Develop a fraud information sharing program that defines what information is shared, with whom it is shared and the rules for using the data
C-3	Security and data privacy permissions on the storage, access and transmission of data	<ul style="list-style-type: none"> • Ensure that all information submitted by stakeholders is appropriate, secure and not misused • In transit and at rest • Access and provisioning aligned with least privileged and validated credentials • Conceptual framework development

Area of Focus: D – Payment Network Rules and Regulations

Work Group Topic		Work Group Objective
D-1	Coordination for rules, regulations, regulators	Identify the gaps in existing roles that present security concerns and engage with the applicable regulatory agencies to align with payment modernization in a coordinated approach
D-2	Managing data in network rules	Produce / data security guidance
D-3	Aligning incentive approaches	Develop an approach to create incentives for stakeholders to broadly adopt the payment networks security standards

Areas of Focus and Potential Work Groups

Next Steps Steering Committee Review

Timeline	Proposed Actions
Sep 24	<u>Organize SPTF Aug 26 Meeting Output.</u> Fed staff will organize SPTF August meeting output into high priority issues and potential work group ideas for Steering Committee review at its Oct 1-2 meeting.
Oct 1-2	<u>Steering Committee Review.</u> SPTF Steering Committee will review areas of focus and high potential work group ideas and prepare for segment calls for input.
Oct 5-21	<u>SPTF Segment Input.</u> Steering Committee members host segment calls to get input on high potential work groups from Oct 1-2 meeting. Begin to identify potential champions/leaders for the high priority work groups.
Nov 9-10	<u>Seek SPTF Endorsement.</u> Present high priority work group ideas to full Task Force for endorsement. Solicit interest among Task Force members to serve on work groups.
Dec 2015 Jan 2016	<u>Form and launch endorsed work groups.</u>



Advise the Fed

Barb Pacheco

Advise the Fed

Standards and Protocols

- Top three ideas for specific activities or actions the Fed might take to:
 - Identify gaps where security standards are needed and accelerate standards/protocol development.
 - Foster industry-wide adoption of payment security standards and protocols.

Education, Outreach, and Research

- Top three topics or problems that would benefit most from Fed involvement in education and outreach, or academic/policy research.

NEXT STEPS

- Organize August Task Force meeting output and share with Steering Committee and Task Force
- Initiate Fed staff review of ideas and identify implementation issues and opportunities and report back to Task Force
- Collaborate with Task Force and others to implement as appropriate



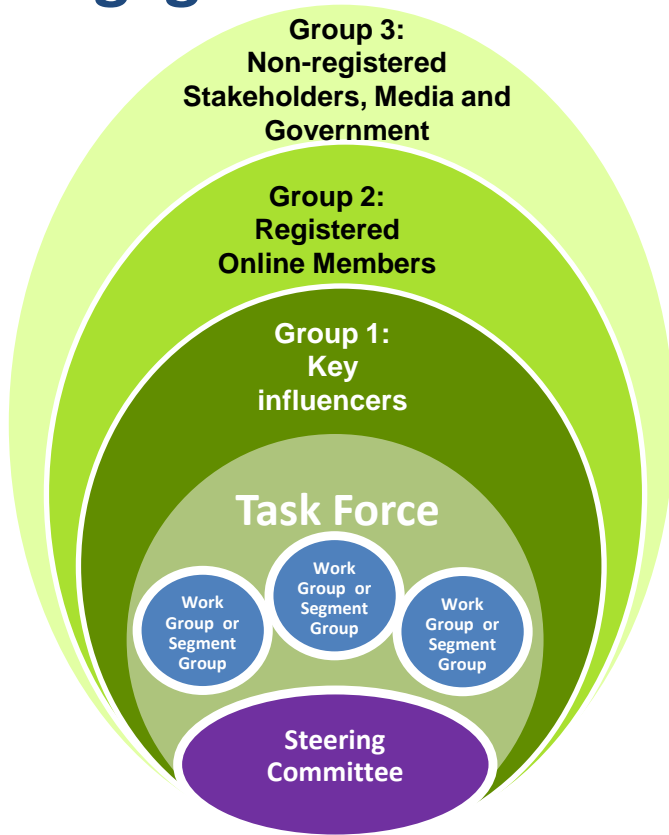
Engagement Planning and Identifying Task Force Education Needs

Connie Theien

Engagement Plan Overview

A plan for facilitating interaction with task force members and broader stakeholder communities to ensure desired levels of awareness, support and engagement, contributing to successful task force outcomes

Engagement Audiences



Plan Deliverables

1. Engagement Framework
2. Content Management
3. Analytics
4. Tools and Technology

Identifying Task Force Education Needs

- On what topics would you like training / education?
- Are you expert in a topic area and willing to provide or assist with Task Force education?

Feedback Mechanisms

Provide live feedback during the call via the Webinar Tool.

Provide feedback via email by sending your responses to SecurePaymentsTaskForce@chi.frb.org

Opportunities and Resources

- Pre-Reading List from August 25-26 Meeting (Appendix)
- Attend *How Can I Weigh-In on Requirements for a Faster Payment System?*
[Webinar](#) September 18 – 12-1:00 p.m. ET

Upcoming Meetings and Deliverables

Upcoming Meetings

- ❑ October 1-2: Steering Committee in-person meeting (FRB Dallas)
 - ✓ Oct 1 10:00 a.m. -- 8:30 p.m. EST, Oct 2 9:00 a.m.—3:00 p.m. EST
- ❑ November 9-10: Full Task Force in-person Meeting (Chicago)
 - ✓ Nov 9 11:00 a.m. – 8:30 p.m. EST, Nov 10 9:00 a.m. – 3:00 p.m. EST
- ❑ December 10 – Steering Committee Teleconference
 - ✓ 1:00 – 3:00 p.m. EST

Deliverables In-Process

- ✓ Glossary of Terms –To be posted on Fedpaymentsimprovement.org
- ✓ Task Force and Community Engagement Plan



Questions?



Appendix

Secure Payments Task Force

Pre-Reading for First In-Person Task Force Meeting

In an effort to leverage existing research on secure payments efforts and prepare for the first in-person meeting, the Federal Reserve expects all Task Force participants to read the following studies.

Secure Payments Research

1. [Strategies for Improving the U.S. Payments System \(Appendix 5. Payment Security Landscape Study, pp. 32-36\)](#)
2. [The 2013 Federal Reserve Payments Study \(section 2.8, Third-Party Payments Fraud, pp. 32-37\)](#)
3. [The Economics of Retail Payments Security](#)
4. [Mobile Payments Industry Workgroup Meeting Discussion on Tokenization Landscape in the U.S.](#)
5. [Controlling Security Risk and Fraud in Payment Systems](#)
6. [Understanding Risk Management in Emerging Retail Payments](#)
7. [Consumer Use of Fraud Alerts and Credit Freezes: An Empirical Analysis](#)
8. [Heartland Payment Systems: Lessons Learned from a Data Breach](#)
9. [The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches](#)
10. [Update on the Cybersecurity Framework](#)