Ensuring Payment Security in the United States

Payment Security Roundtables

June 5, 11, and 18, 2014

Barb Pacheco
Federal Reserve Bank of Kansas City
Customer Relations and Support Office

Connie Theien
Federal Reserve Bank of Chicago
Customer Relations and Support Office

Payment Security Roundtable Agenda

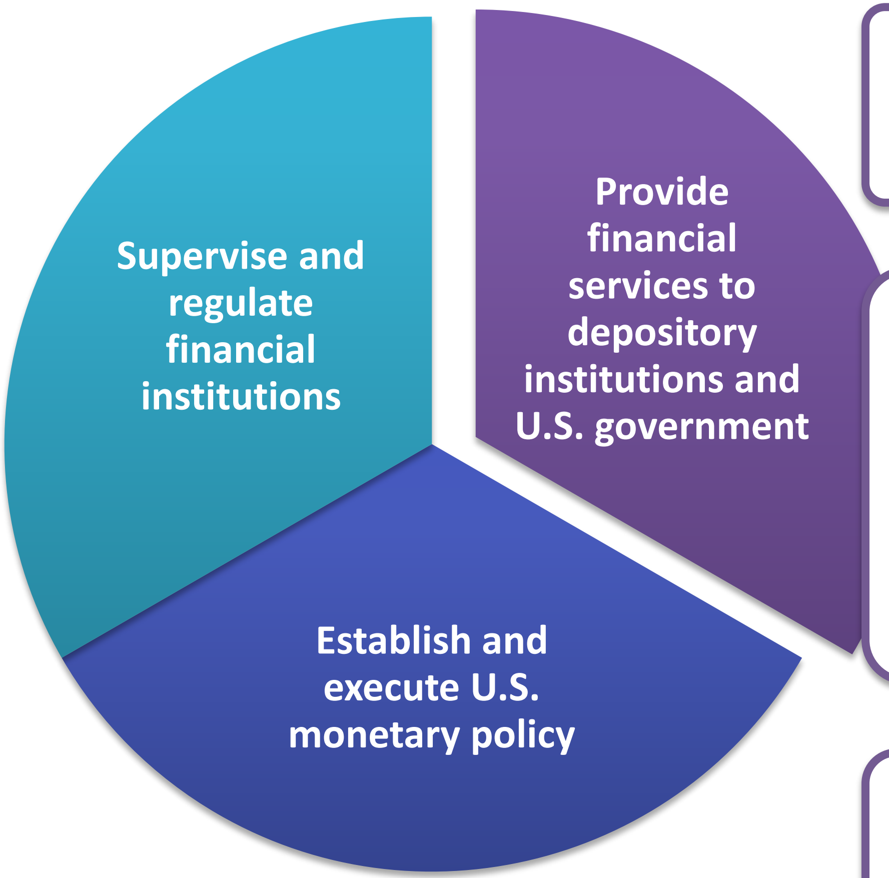
- Part I
  - Review Federal Reserve Banks' Strategic Direction and Desired Outcomes for the U.S. Payment System
  - Share Federal Reserve Payment Security Landscape Study approach and learnings
  - Discuss U.S. payment security weaknesses and opportunities for improvement and roundtable participants' views on priorities for action
- Part II
  - Share initial ideas for how the Federal Reserve might support industry progress toward the desired outcome for payment security
  - Discuss roundtable participants' views on these U.S. payment security improvement concepts, additional payment security improvement strategies
  - Discuss the role of the Fed and other payments system stakeholders
- Next Steps

Federal Reserve Banks

Strategic Direction for Financial Services

BACKGROUND

Federal Reserve System Overview



Supervise and regulate financial institutions

Provide financial services to depository institutions and U.S. government

Establish and execute U.S. monetary policy

…to maintain a stable financial system and contain systemic risk

Federal Reserve Financial Services Mission

- To foster integrity, efficiency and accessibility of the U.S. payment system

Federal Reserve Financial Services Vision

- Payments are safe and efficient
- End users can select payment options with attributes (e.g., speed, convenience, cost, security) that meet their needs
- Incentives promote efficient selection and use of these options

Federal Reserve Banks’ Role in Payments

- Act as a major service provider to the interbank market
- Collaborate with stakeholders and emphasize innovations in electronic payment systems

A New End-to-End Strategic Focus

Safety and Security

- Maintain and enhance Federal Reserve Financial Services network security
- Enhance understanding of end-to-end security
- Collaborate and promote industry best practices

Speed

- Develop solutions to enhance payment speed
- Understand market demand for faster payments
- Continue migration of paper to electronic

Efficiency

- Develop solutions to promote efficiency
- Understand needs and barriers
- Promote standards adoption to improve efficiency

Five Desired Outcomes will Guide U.S. Payment System Improvements

A ubiquitous, faster electronic solution(s) exists for making a broad variety of business and personal payments, and the Federal Reserve provides a flexible and cost-effective means for private sector arrangements to settle their positions rapidly and with finality.

Greater electronification of payments originated and received has reduced the average end-to-end (societal) costs of payment transactions and resulted in innovative payment services that deliver improved value to consumers, businesses and governments.

Consumers and businesses have better choice in making convenient, cost-effective and timely cross-border payments from and to the United States.

U.S. payment system security is very strong, public confidence in it is high and protections and incident response have kept pace with the rapidly evolving and expanding threat environment.

Key improvements for the future state of the payment system have been *collectively* identified and embraced by a broad array of payment participants, and material progress has been made in implementing them.

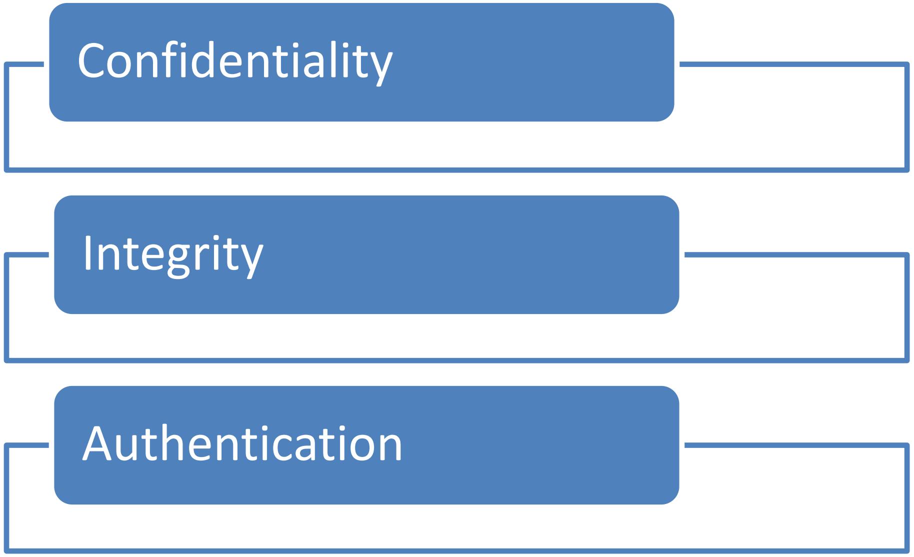
Federal Reserve Banks

Payment Security Landscape Study

APPROACH AND KEY LEARNINGS

Payment Security Landscape Study Objective, Definition and Scope

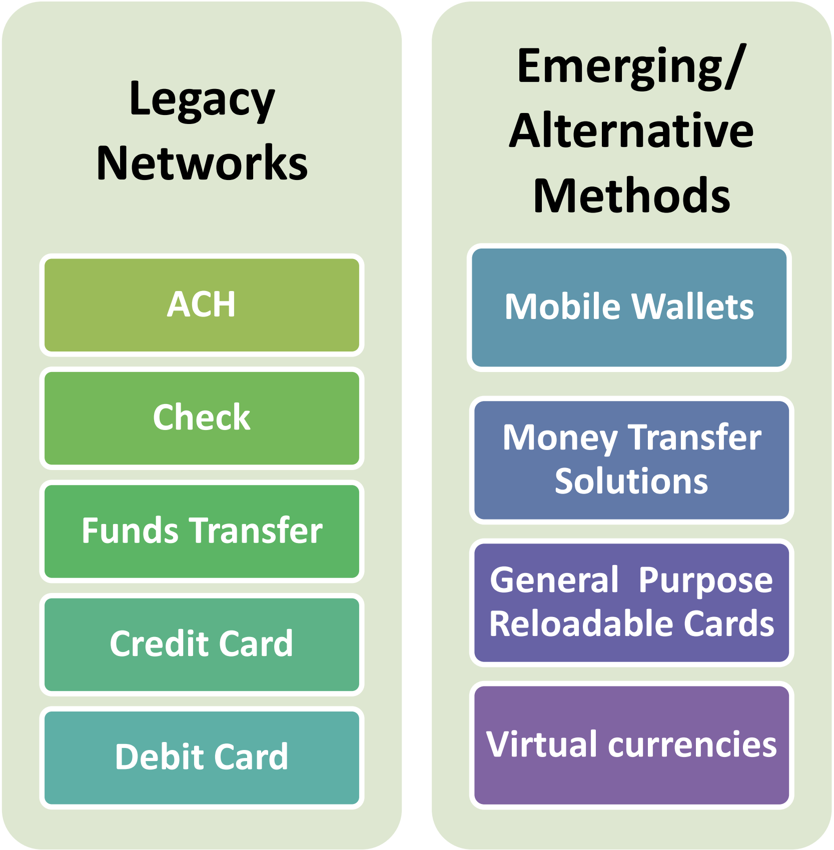
The Payment Security Landscape Study (PSL Study) was undertaken to enhance our understanding of end-to-end payment security and identify opportunities for improving it in collaboration with payment system stakeholders.



Confidentiality

Integrity

Authentication



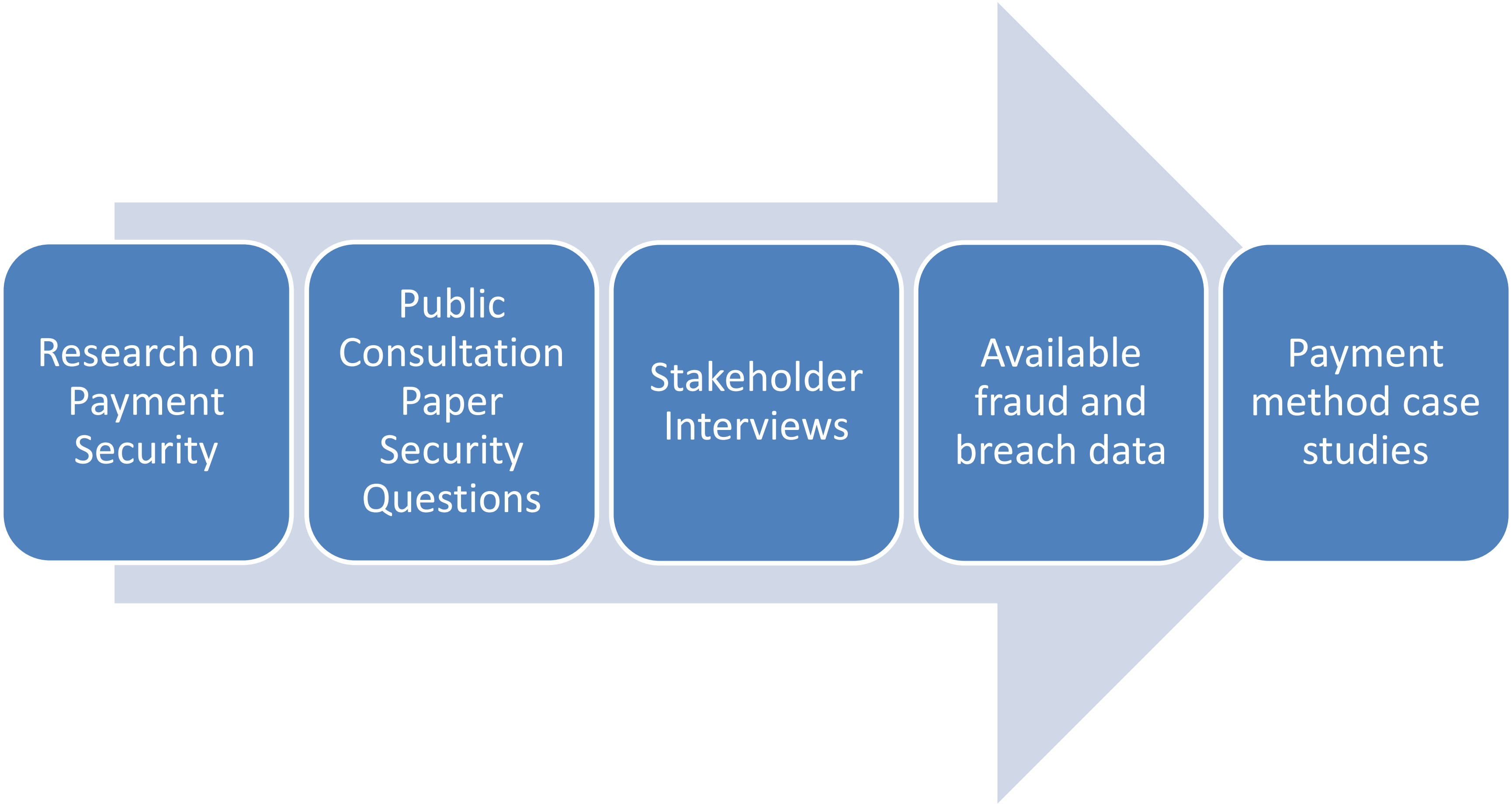
Legacy Networks

- ACH
- Check
- Funds Transfer
- Credit Card
- Debit Card

Emerging/ Alternative Methods

- Mobile Wallets
- Money Transfer Solutions
- General Purpose Reloadable Cards
- Virtual currencies

PSL Study Sources of Information



Research on Payment Security

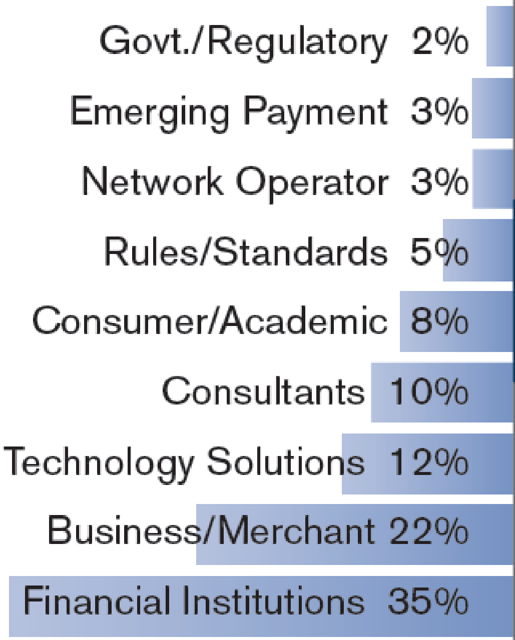
Public Consultation Paper Security Questions

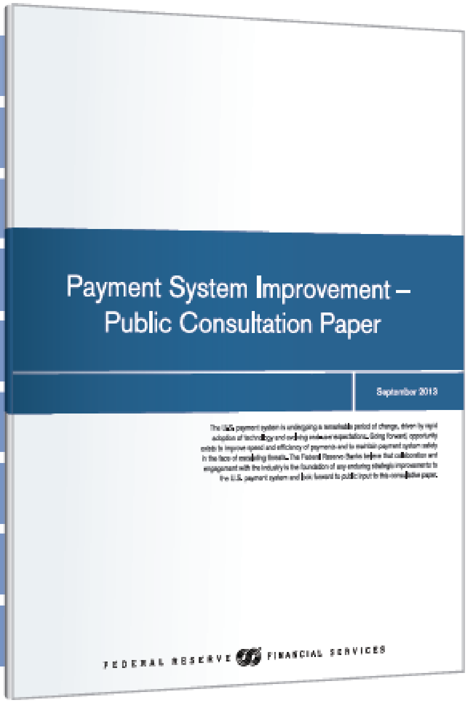
Stakeholder Interviews

Available fraud and breach data

Payment method case studies

Federal Reserve Banks' *Public Consultation Paper* Responses to Payment Security Questions




Payment System Improvement – Public Consultation Paper

September 2013

The U.S. payment system is undergoing a remarkable period of change, driven by rapid adoption of technology and evolving end-user expectations. Going forward, opportunity exists to improve speed and efficiency of payments and to maintain payment system safety in the face of escalating threats. The Federal Reserve Banks believe that collaboration and engagement with the industry is the foundation of any enduring strategic improvements to the U.S. payment system and look forward to public input to this consultation paper.

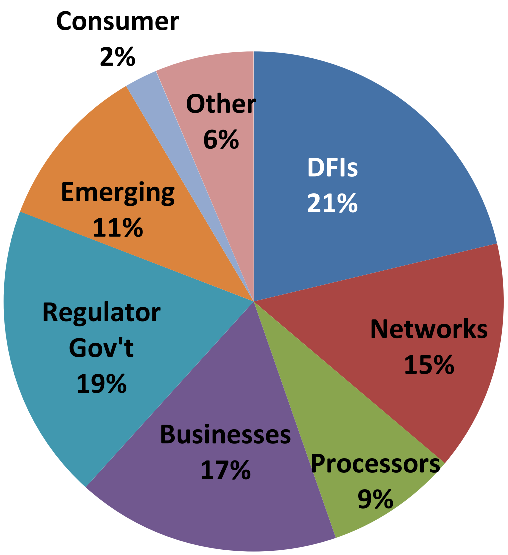
FEDERAL RESERVE FINANCIAL SERVICES

- Respondents suggest the industry work together to develop new fraud prevention tools
- Many also advocated for the development and adoption of security standards
- Many believe consumers need better education and incentives to make fraud-reducing payment choices

Key Findings from 40 PSL Study Interviews

- The payment system faces **persistent and ever-changing threats.** Participants are placing a **high priority on improving authentication** of parties and equipment in the payment process and are **actively pursuing the protection of sensitive information** and **limiting its use and availability** for perpetrating fraud.
- **Information sharing and data analysis are important** to participants in mitigating the adverse impact of these threats on payment system security.
- Private and public sector stakeholders in the payment system have **increased the focus and priority on security,** making additional resources available to strengthen it.

Interviewee Composition



- Innovative and advanced technology is available to strengthen payment security; however, the complexity and sheer number of endpoints that comprise the U.S. payment system make **coordination challenging** and payment system-wide **adoption of improved security technologies a time and resource-intensive** endeavor.
- As nonbanks become more prominent in the electronic payments process, **regulators are reassessing their supervision and enforcement approaches** accordingly and activities to redirect resources and build expertise are underway.

Industry Perspectives on Role of the Fed

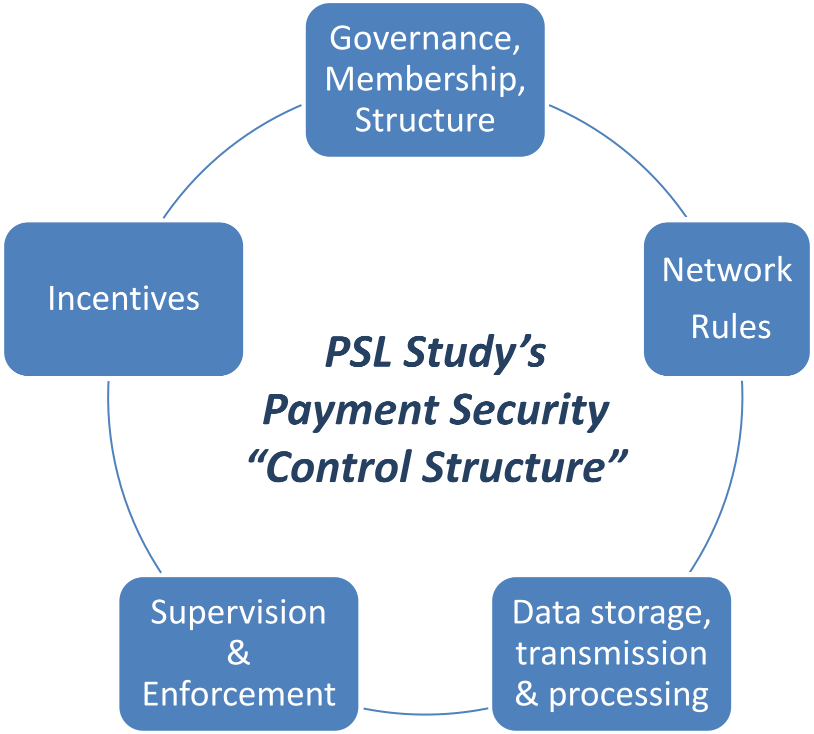
The most common view across stakeholders regarding the roles the Fed should play to strengthen payment security is as **leader, catalyst and convener**. Specific examples include:

- The Fed's unique ability to bring parties with diverse viewpoints together to think about the broader payment system.

- The quality and objectivity of the Fed's research capabilities were mentioned as valuable.

- The relationships with public authorities and regulators position the Fed to initiate discussions that might encourage clarity on payment security requirements and expectations across the various participants and payment systems.

Key Takeaways from Case Studies


Governance, Membership, Structure
Network Rules
Data storage, transmission & processing
Supervision & Enforcement
Incentives
PSL Study's Payment Security "Control Structure"

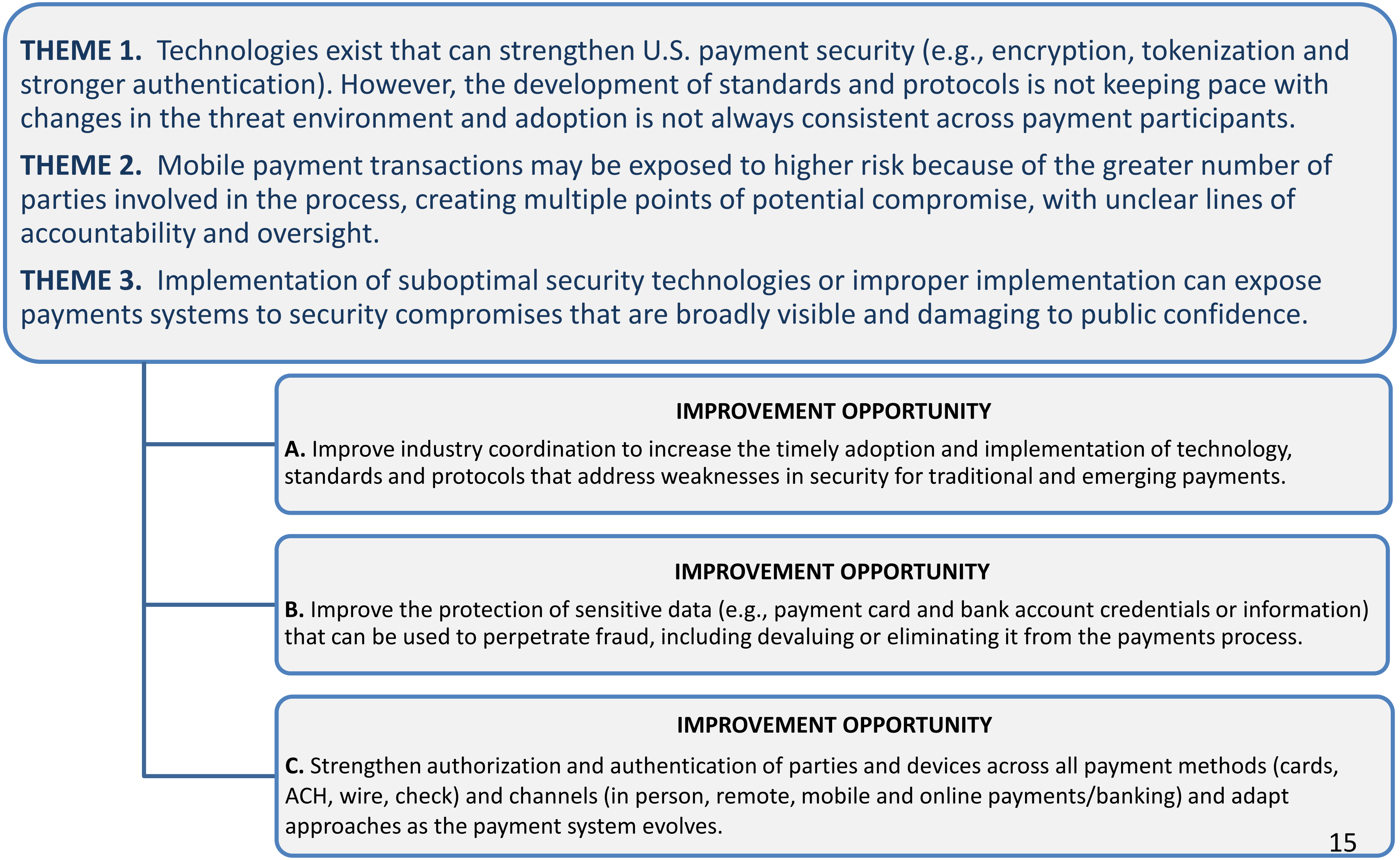
- ❖ Importance of incentives – payment security is the result of efforts of all parties based on their assessment of private costs and benefits
- ❖ Fraud cost allocation and consequence of data breaches
- ❖ Key technology (development/ selection by networks and adoption by other participants)
- ❖ Competition and collaboration on payment security; how standards and practices are established
- ❖ Legal and regulatory uncertainty

Federal Reserve Banks

Payment Security Landscape Study

SUMMARY OF WEAKNESS THEMES & IMPROVEMENT OPPORTUNITIES

Weakness Themes and Improvement Opportunities



THEME 1. Technologies exist that can strengthen U.S. payment security (e.g., encryption, tokenization and stronger authentication). However, the development of standards and protocols is not keeping pace with changes in the threat environment and adoption is not always consistent across payment participants.

THEME 2. Mobile payment transactions may be exposed to higher risk because of the greater number of parties involved in the process, creating multiple points of potential compromise, with unclear lines of accountability and oversight.

THEME 3. Implementation of suboptimal security technologies or improper implementation can expose payments systems to security compromises that are broadly visible and damaging to public confidence.

IMPROVEMENT OPPORTUNITY

A. Improve industry coordination to increase the timely adoption and implementation of technology, standards and protocols that address weaknesses in security for traditional and emerging payments.

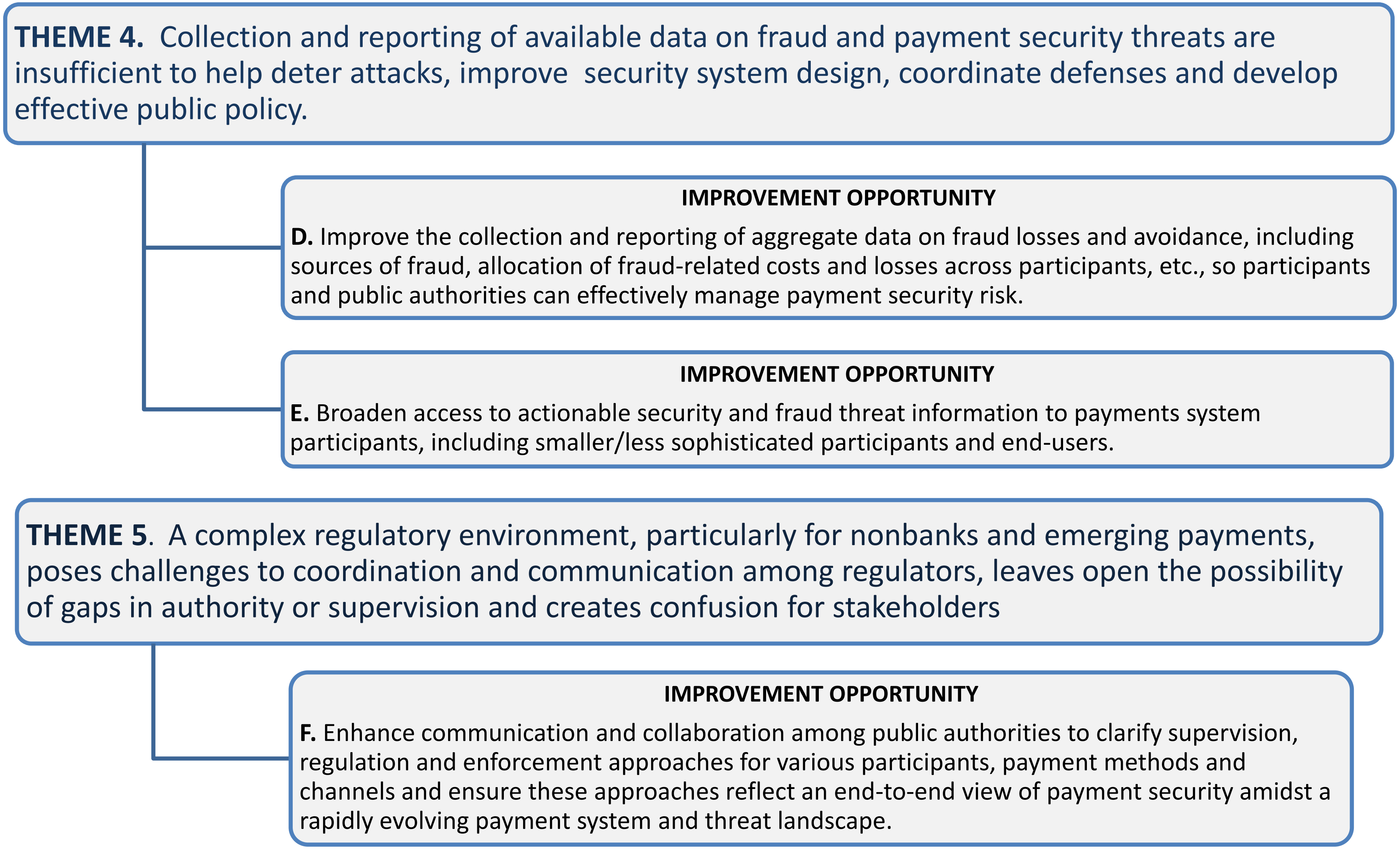
IMPROVEMENT OPPORTUNITY

B. Improve the protection of sensitive data (e.g., payment card and bank account credentials or information) that can be used to perpetrate fraud, including devaluing or eliminating it from the payments process.

IMPROVEMENT OPPORTUNITY

C. Strengthen authorization and authentication of parties and devices across all payment methods (cards, ACH, wire, check) and channels (in person, remote, mobile and online payments/banking) and adapt approaches as the payment system evolves.

Weakness Themes and Improvement Opportunities



THEME 4. Collection and reporting of available data on fraud and payment security threats are insufficient to help deter attacks, improve security system design, coordinate defenses and develop effective public policy.

IMPROVEMENT OPPORTUNITY

D. Improve the collection and reporting of aggregate data on fraud losses and avoidance, including sources of fraud, allocation of fraud-related costs and losses across participants, etc., so participants and public authorities can effectively manage payment security risk.

IMPROVEMENT OPPORTUNITY

E. Broaden access to actionable security and fraud threat information to payments system participants, including smaller/less sophisticated participants and end-users.

THEME 5. A complex regulatory environment, particularly for nonbanks and emerging payments, poses challenges to coordination and communication among regulators, leaves open the possibility of gaps in authority or supervision and creates confusion for stakeholders

IMPROVEMENT OPPORTUNITY

F. Enhance communication and collaboration among public authorities to clarify supervision, regulation and enforcement approaches for various participants, payment methods and channels and ensure these approaches reflect an end-to-end view of payment security amidst a rapidly evolving payment system and threat landscape.

Discussion Questions: Weakness Themes and Related Improvement Opportunities

- Do you agree with the Study's conclusions on payment system security weaknesses and opportunities for improvement?
- What is the impact on your organization and its customers if these weaknesses persist?
- What are the most important activities underway to address these issues and what are the barriers and/or prospects for their success?
- What is your view of the impact of each of these weaknesses on the public's confidence in electronic payments?
- How would you prioritize these issues for action?

Federal Reserve Banks

Payment Security Landscape Study

DESIRED OUTCOME FOR PAYMENT SECURITY AND PROPOSED IMPROVEMENT CONCEPTS

U.S. Payment Security Desired Outcome

U.S. payment system security is very strong, public confidence in it is high and protections and incident response have kept pace with the rapidly evolving and expanding threat environment.

Summary of Feedback from Roundtable Participants

Desired Outcomes and Weaknesses/Opportunities for Improvement

- Participants generally agreed with the desired outcome for payment security and voiced concern that public confidence in the payment system is at risk.
- There was agreement on most, but not all, of the weakness themes. Most agreed that development of standards was too slow, but overcoming barriers to broad adoption was the larger concern.
- There was strong support for the need to improve authentication and devalue or remove static payment information.
- They agreed the regulatory landscape is complex and may not offer a level playing field for all market participants.
- A number of participants objected to highlighting mobile payments as a separate risk rather than digital commerce or card-not-present transactions more generally.
- Some participants agreed with the lack of good data on payment fraud, while others were less certain of its incremental value.
- Participants agreed with weaknesses in information sharing noting several barriers.

Concept #1: Establish a Payment Security Advisory Council

Description	Establish an executive level advisory council on payment security with Federal Reserve System leadership and representation from all stakeholders to discuss issues and form consensus on how best to address them.
Discussion Questions	1. What kind of leadership, charter and membership is necessary to be successful in gaining consensus on the most important issues impacting the strength of payment security? 2. What are the high level benefits and considerations of establishing a U.S. payment security council to set a broad roadmap for strengthening payment security that would be beneficial to standards and other efforts? 3. What are the highest priority issues you believe should be discussed or overseen by such a council? 4. Are there examples of similar councils in other countries that we should learn from?

Concept #1: Roundtable Feedback

Summary

- Membership should be at the highest level possible for decision-making/influence and business commitment. Members are to be advised by technical executives. All stakeholders must be represented, with rotation of members and recalibration (new participants) as industry changes.
- While senior executives are key for buy-in and funding, knowledgeable payment security executives should be engaged in working groups (existing or new as needed) to make recommendations.
- Challenges include translating talk to action, overcoming divergent interests and optimizing group size.
- Fed leadership has been successful in the past, and Fed involvement may add credibility. The Fed serving in the convener role appears to be influential in faster payments. The Fed may need to seek authority, use regulatory authority or consider other incentives for action.

Overall Conclusion

- There was broad agreement in establishing a council that provides an equal voice for stakeholders to influence payment direction. This will require clarity of objectives and overcoming skepticism about the council’s ability to reach agreement or take action.
- Establishment of a payment security advisory council will be needed as a supporting tactic to accelerate development and broad adoption of payment security standards.

Concept #2: Develop a Mobile Payment Security Framework

Description	Expand current collaborative effort with Mobile Payments Industry Work Group (MPIW) to develop a mobile/digital payments end-to-end security framework.
Discussion Questions	1. What are the key security issues and gaps (technology or business practice) for mobile/digital payments? Authentication and authorization protocols, end-to-end mobile payment process, customer data ownership, data security, consumer protection/privacy, other? 2. What is your sense of the extent of agreement in the industry on the most important mobile payment security issues? 3. Are potential solutions different based on underlying funding payment method (e.g., cards, ACH, pre-funded account, etc.)? Or, can there be a common framework or approach for all mobile-initiated payments? 4. Are current laws and regulations regarding who is responsible and the appropriate resolution of mobile payment fraud sufficient? If not, what changes should be made?”

Concept #2: Roundtable Feedback

Summary

- Some participants agreed that uniqueness of the form factor and the present timing (before a dominant approach has developed) are factors that support a strategy to specifically focus on mobile payment security.
- More participants noted, though, that a holistic approach to a payment security framework that accounts for all form factors (including mobile/digital), channels and methods may be more useful and durable.
- Mobile devices may introduce incremental risks but also offer potential solutions to combat fraud.
- Data ownership and data sharing are issues to be addressed.
- MPIW has been a helpful group to bring innovators together with other participants and to engage all participants.

Overall Conclusion and Strategy Implications/Adjustments

- While attention on mobile/digital payments is appropriate, a number of participants suggested that development of a broader framework of standards and principles for payment security would be preferable. This concept may be best merged into a broader strategy to accelerate development and broad adoption of payment security standards. Specific work on mobile/digital payment security should continue through existing MPIW efforts.

Concept #3: Payment Security Industry Standards Development

Description	Work with payment system stakeholders to accelerate development and adoption of payment security standards and related business processes.
Discussion Questions	1. What are the top priorities for security standards and business process development? Tokenization, point-to-point encryption, end-to-end encryption, authentication (in-person and remote)? 2. What are the key barriers/factors that prevent the industry from accelerating development and adoption of security standards that need to be considered? 3. What can the Fed do to assist in accelerating development and adoption of security standards? Increase participation in open standards efforts? Provide leadership and/or convene stakeholders to forge consensus? Other roles? 4. What should the Fed ***not*** do?

Concept #3: Roundtable Feedback

Summary

- Participants expect Fed involvement in open standards. Proprietary standards limit competition, interoperability and merchant/issuer choices.
- PCI will continue to have a powerful influence, and new security developments will have to live in harmony with PCI. Global views and interoperability are also considerations.
- Participants most supported addressing authentication and tokenization standards and encryption standards secondarily. Design should account for end-user behavior and incentives.
- Some believe we have the standards we need, while others think we may need more standards. All agree, though, on the need to enforce standards.

Overall Conclusion and Strategy Implications/Adjustments

- There was broad and strong agreement for this concept, with particular attention to involvement in open standards. Other concepts discussed during the roundtable may be viewed as supporting tactics to this broader strategy to accelerate development and broad adoption of payment security standards.

Concept #4: Fraud Data Collection and Reporting

Description

Lead a collaborative effort with stakeholders to improve the quality, consistency and value of payment fraud data collected and reported.

Discussion Questions

1. Does your organization monitor incidents and losses due to payment fraud? If so, what information and processes do you use to track and classify payment fraud?

2. What benefits would you anticipate for the payment industry and for policymakers if we had better statistics on payment fraud?

3. What are some of the challenges your organization sees in collecting and reporting fraud data so that it can be aggregated for broader industry research?

4. What data is valuable to you – your own data, aggregate data of your peers, industry-wide data?

Concept #4: Roundtable Feedback

Summary

- Participants urged careful thought on measurements, definitions, granularity and frequency.
- The benefit of data collection and reporting should be explained (to justify burden/cost).
- Data can provide useful insight for benchmarking and policy; however, whether the data will lead to action was a question.
- Participants are sensitive about sharing information unless it is anonymized. Additionally, there is a need to address legal barriers to information sharing.
- Some participants indicated greater support for developing and disseminating timely information on fraud schemes, breaches and threats versus the periodic publication of aggregate fraud statistics.

Overall Conclusion and Strategy Implications/Adjustments

- Support for this concept was divided. Some argued that objective data would be beneficial for policy decisions and benchmarking, while others expressed skepticism about whether the data would lead to action. Improving fraud data collection and reporting is a supporting tactic to garner high-level support for principles and standards, to overcome barriers to adoption and to track progress on payment security goals.

Concept #5: Federal Reserve System Payment Security Research

Description

Expand Federal Reserve System capacity to deliver payment security research that anticipates future payment security challenges and is highly valued by policy makers and industry stakeholders.

Discussion Questions

1. What research topics or questions do you believe will support strategies and decisions by payment system participants that ensure strong payment security and good public policy? Examples:

- Incentives
- Cost/benefit analysis
- Fraud analysis/reporting
- Standard setting issues and impacts
- Market impact of regulatory policy on competition and security

2. How receptive do you think the industry will be to supporting Federal Reserve research on payment security by sharing data, technical expertise, institution-level details?

Concept #5: Roundtable Feedback

Summary

- Participants offered numerous ideas for research topics including: the impact of various technologies on fraud and data compromises; the extent of security measures adoption; the security of anonymous payments; measuring reputational risk; understanding consumer behavior; comparing security via product design vs. education; and documenting incentives in the payment system, among many others.
- In addition to publishing academic papers, other more timely and accessible publications would also be helpful.
- The Fed could create a network of outside academic affiliations to obtain more research on payment security.

Overall Conclusion and Strategy Implications/Adjustments

- General agreement: Participants were supportive of enhancing research in payment security, and some participants expressed willingness to provide their support to Fed researchers (e.g., by participating in research or helping make connections to those with data). The Fed should focus specific resources on payment security research as a supporting tactic in conjunction with improving data collection and reporting.

Discussion on Other Payment Security Improvement Ideas and Priorities for Action

- Are there other strategies that the Fed and/or payment system participants should pursue to achieve the desired outcome?
- How would you prioritize these? If you had to choose one initiative to advance, which would you choose and why?
- What is the appropriate Fed role in ensuring U.S. payment security? Roles of other organizations with a public interest in payment security?

Summary of Feedback from Roundtable Participants

Strategies to Improve Payment Security

- Many participants voiced strong support for two strategies:
  - 1) to accelerate development and adoption of payments security standards (authentication and tokenization)
  - 2) to establish a high level council, giving all stakeholders a voice in the direction of payment security.
- They indicated that success rests on the ability to enforce or create other incentives to adopt open standards and whether the council will have the appropriate level of authority, influence or moral suasion for a consensus on direction to be effective.
- Many suggested regulatory guidance or other tactics to strengthen payment security across channels and types, although a few raised concerns that mandates could slow innovation and reduce competition.
- There was mixed support for developing a mobile payment security framework. Some participants acknowledged mobile was unique in some respects, while others suggested a more holistic approach to strengthening security across all form factors and channels.
- Some participants valued more timely fraud and threat data over aggregate fraud data. Many commented, however, on the barriers (e.g., liabilities, risks) that prevent data sharing and the need to address these for a data collection/sharing strategy to be successful.
- There was general support for additional Fed research on payment security with an eye to preparing for the next major data breach or incident that will lead policy makers to seek its advice.

Next Steps

Prepare and Share a Roadmap
Using industry input and research insight, prepare and share a roadmap for payment system improvement initiatives that advance the speed, efficiency and security of payments

Collaborate to Achieve Desired Outcomes
Engage inddustry stakeholders in advisory roles and working groups to design and implement roadmap initiatives

Visit FedPaymentsImprovement.org to stay connected!