Payments Security Panel

CHICAGO
PAYMENTS SYMPOSIUM

An industry leader dialogue hosted by
the Federal Reserve Bank of Chicago

The Federal Reserve Banks'

PAYMENT SECURITY LANDSCAPE STUDY

Context for the Federal Reserve Banks' Payments Security Landscape Study

- Mission is to promote the integrity and efficiency of the payments system and to ensure the provision of payment services to all depository institutions on an equitable basis, and to do so in an atmosphere of competitive fairness.

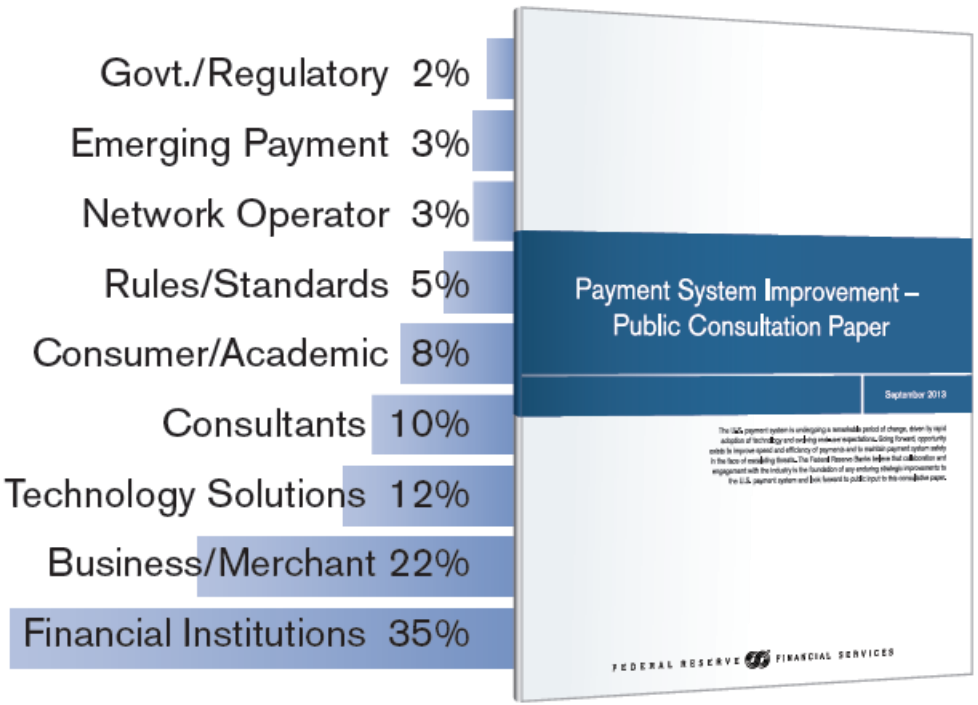
  The Federal Reserve in the Payments System (1984, rev. 1990)

- Federal Reserve Financial Services Strategic Direction

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

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

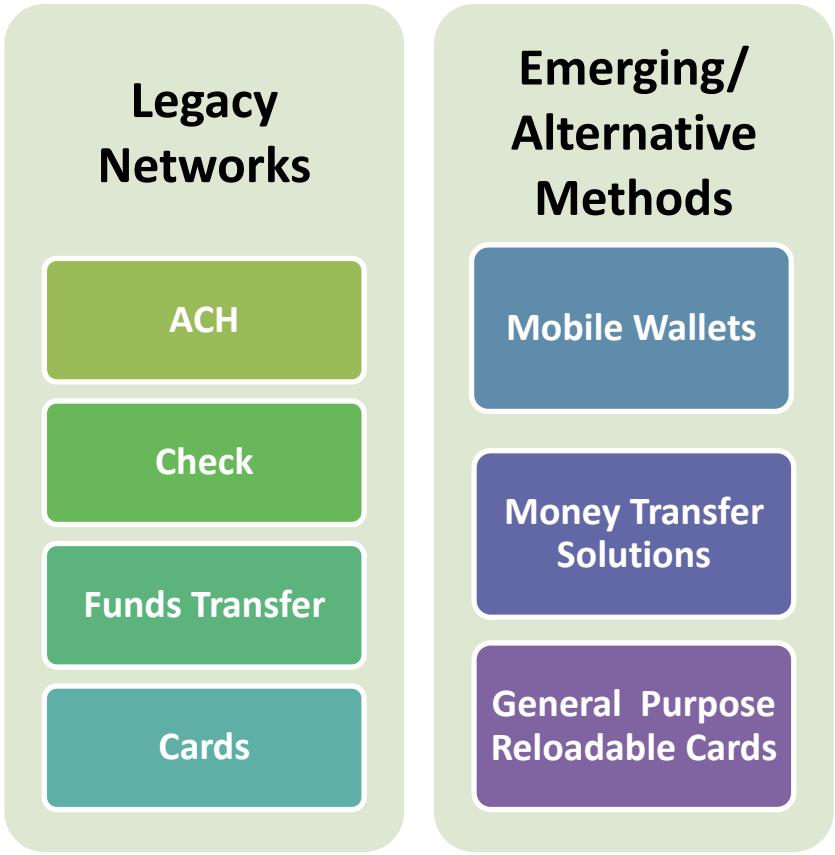


- Respondents suggest the industry work together to develop new fraud prevention tools
- Many also advocated for the development and adoption of security standards
- Many believe consumers need better education and incentives to make fraud-reducing payment choices

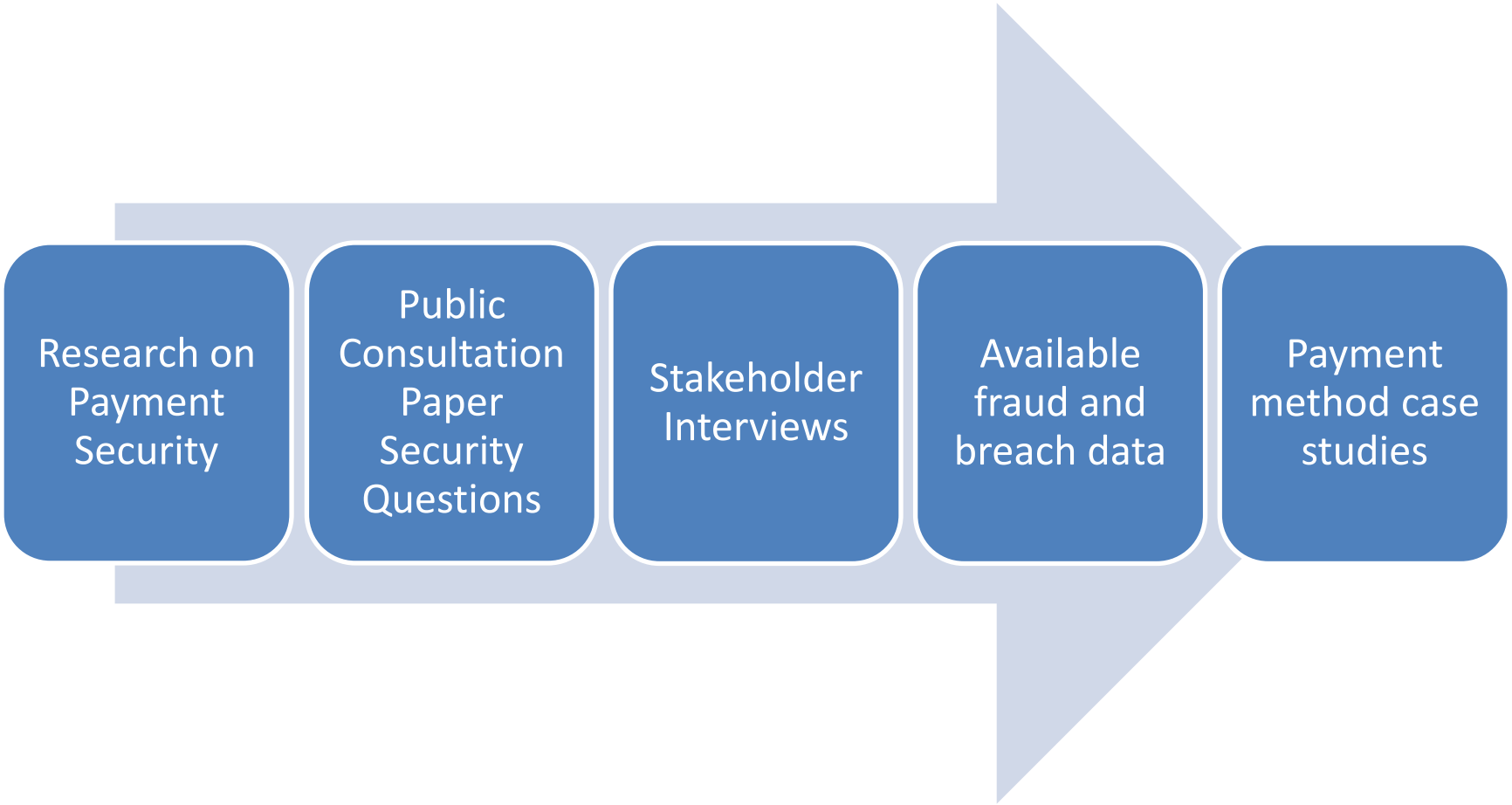
Payment Security Landscape Study Objective, Definition and Scope

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



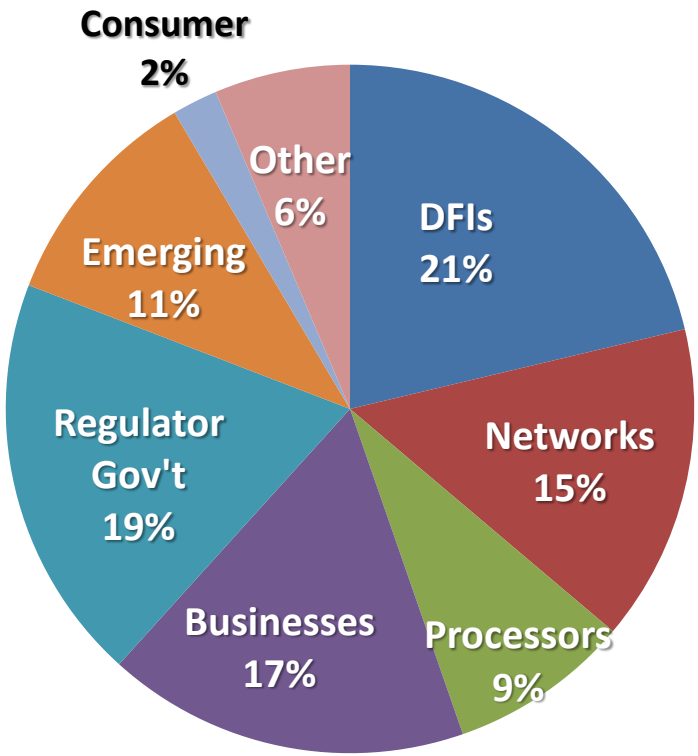
PSL Study Sources of Information



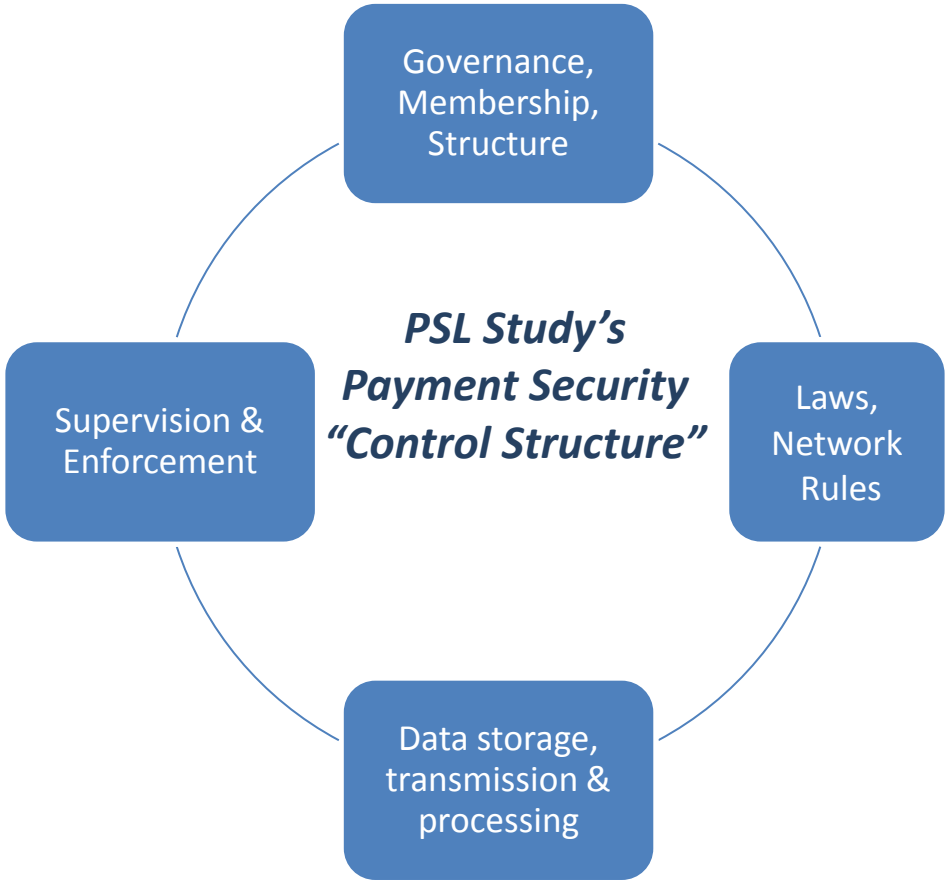
Key Findings from 40 PSL Study Interviews

- The payment system faces persistent and ever-changing threats.
- Priorities include improving authentication, protecting sensitive information and limiting its use and availability for perpetrating fraud.
- The complexity and number of endpoints introduce coordination challenges in development and adoption of improved security technologies.
- Fraud and threat information sharing and data analysis are in high demand.
- As new payment methods and players emerge, regulators are reassessing their supervision and enforcement approaches. Activities to redirect resources and build expertise are underway.

Interviewee Composition



Key Takeaways from Case Studies



- ❑ 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

Weakness Themes and Improvement Opportunities

THEME 1: Standards Development and Adoption

Development of security standards and protocols is not keeping pace with changes in the threat environment and adoption is not always consistent across payment participants.

THEME 2: Security Technology Implementation Issues

Implementation of weak security technologies or improper implementation can expose payments systems to security compromises that may damage public confidence.

Improve industry coordination to increase the timely adoption and implementation of technology, standards and protocols.

Improve the protection of sensitive data that can be used to perpetrate fraud and devalue or eliminate it from the payments process.

Strengthen authorization and authentication of parties and devices across all payment methods and channels and adapt approaches as the payment system evolves.

Weakness Themes and Improvement Opportunities

THEME 3: Data Collection, Sharing and Reporting

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.

Improve the collection and reporting of aggregate data on fraud losses and avoidance, sources, allocation of costs and losses among participants, so participants and public authorities can effectively assess and manage payment security risk.

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

Weakness Themes and Improvement Opportunities

THEME 4: Complex Regulatory Environment

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

Enhance communication and collaboration among public authorities to clarify supervision, regulation and enforcement approaches and ensure they reflect an end-to-end view of payment security amidst a rapidly evolving payment system and threat landscape.

Discussion Questions: Payments Security Improvement

1. Do you agree with the Study's conclusions on payment system security weaknesses and opportunities for improvement?

   - ❑ What is missing?

2. What are the most important initiatives that are underway or might be taken to address these issues?

   - ❑ What are the barriers and/or prospects for their success?

3. How would you prioritize these issues for action?

4. What can/should the Federal Reserve do to support these payments security improvements?