Research Results Summary

Payment Security Landscape Study

In alignment with their refreshed strategic direction, the Federal Reserve Banks proposed five desired outcomes to be achieved to address the gaps and opportunities identified in the "Payment System Improvement – Public Consultation Paper." The Payment Security Landscape Study was undertaken to enhance our understanding of end-to-end payment security. The study encompassed documenting the current activities of participants, control systems and threat environment to identify the weaknesses and opportunities to improve the security of the U.S. payment system.

DESIRED OUTCOME
ENHANCED PAYMENTS SAFETY AND SECURITY

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

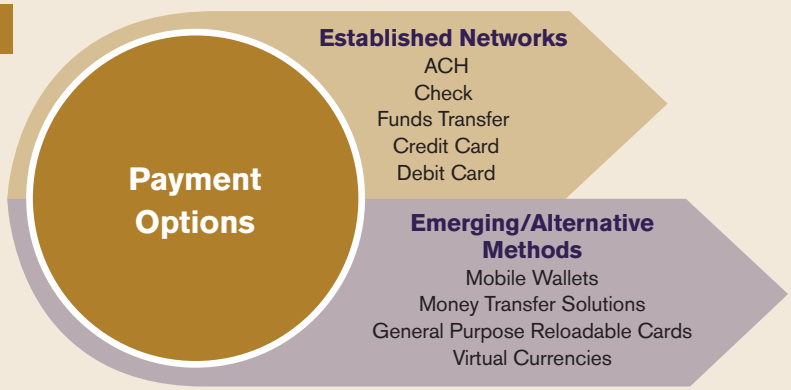
Defnition and Scope

The definition of payment security for purposes of this study incorporated:

Confidentiality: Preserving authorized restrictions on payment information access and disclosure, including the means for protecting personal privacy and proprietary information.

Integrity: Guarding against improper payment message modification or destruction.

Authentication: Ensuring authenticity of counterparties and devices and ensuring links in the chain that authorize, clear and settle payments are all genuine.



The scope of the study includes payment methods on legacy networks as well as emerging/alternative forms in order to address the weakness themes and opportunities in payment system security from end to end.

Key Activities

The study included many sources of information and provided information on current activities directed at payment security improvement and gathered opinions on payment security gaps and barriers to success. A number of themes were prevalent:

- Participants place 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 threats on payment system security.
- Private and public sector stakeholders in the payment system have increased their focus and priority on security, making additional resources available to strengthen it.
- 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 makes 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 payment process, regulators are reassessing their supervision and enforcement approaches accordingly, and activities to redirect resources and build expertise are underway.

Key Takeaways

Challenges to U.S. Payment Security

The payment system faces persistent and ever-changing threats from numerous sources. As payments have become more electronic and threats to payment confidentiality and integrity escalate, challenges in payment security are increasingly acute. Data breaches, phishing attacks, spoofed websites, payment card skimming, fraudulent ATM withdrawals, computer malware and infiltration of retail point-of-sale systems are becoming more prevalent and costly. More options for where and how payments can be initiated are creating growing challenges to authenticate transactions, end users and their devices. As new entrants bring to market innovative payment products and services, new risks may be introduced and must be identified, monitored and managed.

Standards

The current environment for developing payment security standards is complex in a way that creates an uncertain trajectory. While there is progress towards new standards on encryption, authentication and tokenization, there are instances of multiple standards being developed to address the same weakness; it is unclear whether these will be complements or competing substitutes.

Information Sharing

Several barriers to the collection and sharing of payment security data were observed during the course of this study. Observed barriers include the proprietary nature of data; concerns about reputational risk, legal risk and privacy implications; and the tradeoffs between cost and benefits of collecting data that can help participants avoid fraudulent activity.

Security Implementation Considerations

There are a variety of factors that affect the end to end implementation of effective security processes, tools and technologies. Included among them are configuration and maintenance of technology, misalignment of payment stakeholder incentives and increasing complexity and decentralization of new payment platforms.

Weakness Themes and Improvement Opportunities

A review of all study inputs revealed a number of weaknesses in payment security and potential barriers to improvement.

Theme One	Theme Two	Theme Three	Theme Four	Theme Five
Development and adoption of standards and protocols is not keeping pace with technology advances and changes in the threat environment	Mobile payment transactions may be exposed to higher risk because of the greater number of parties in process and unclear lines of accountability and oversight	Suboptimal security technologies or process can result in compromises that are damaging to public confidence	Collection and reporting of available data on fraud and payment security threats are insufficient to help facilitate improvements or prevention **Improvement Opportunities** • Improve the collection and reporting of aggregate data on fraud losses and avoidance • Broaden access to actionable security and fraud threat information to payment system participants	A complex regulatory environment, particularly for nonbanks and emerging payments, poses challenges to coordination and communication among regulators **Improvement Opportunities** • Enhance communication and collaboration among public authorities to clarify supervision, regulation and enforcement approaches for various participants, payment methods and channels that reflect an end-to-end view of payment security

Improvement Opportunities

- Improve industry coordination on timely adoption of technology, standards and protocols
- Improve the protection of sensitive data, including devaluing or eliminating it from the payment process
- Strengthen authorization and authentication of parties and devices across all payment methods and channels

Federal Reserve Banks Strategic Direction in Payments

The Federal Reserve Banks updated their strategic direction in payments in 2012. Our objective is to improve the speed, efficiency and safety of the U.S. payment system from end to end. The analysis reflected in this document is being used to inform improvement strategies to achieve this vision. To advance industry dialogue and gain further insight and commitment to turn this vision into reality, the Federal Reserve Banks continue to engage with all organizations involved in delivering payment services to end users. We believe industry collaboration will be essential to any enduring strategic improvements.

080114CRSO0577