

Achieving Sustainable Improvements in the

# SECURITY OF RETAIL PAYMENTS

Technologies, Standard-Setting, and Coordination

A Conference Sponsored by the Payment Cards Center

February 16 - 17, 2010

## AGENDA



FEDERAL RESERVE BANK OF PHILADELPHIA





In recent years, data breaches at merchants and payment processors have raised concerns about the protection of personal information in the banking and payment industries. The private sector has responded with several attempts to develop ways to better secure these systems, including standard-setting initiatives such as PCI-DSS.

Some stakeholders support specific technology solutions to address specific risks to data security when data are at rest and when data are in transit. In particular, three technology solutions — end-to-end encryption, tokenization, and chip or smart card technology — are frequently suggested.

One objective of this conference is to evaluate these technology solutions: how they function, how they are applied to consumer payment networks, and how well they could meet data security objectives for each participant in the payment chain. But the success of a particular technology may not reside in the technology itself but rather in the ability to broadly implement it among diverse market participants in a cost-effective way.

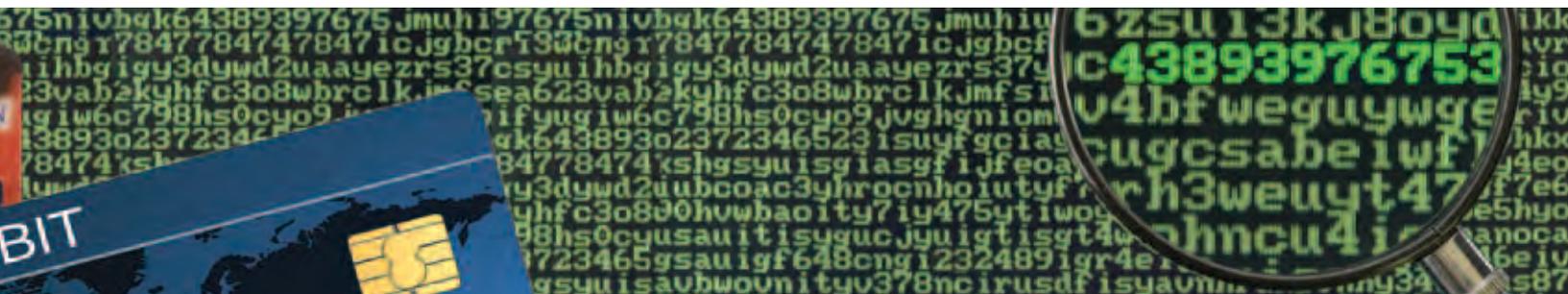
In addition, a set of solutions selected as part of a comprehensive risk management strategy is likely required. This implies a level of coordination — including acceptance, adoption, and enforcement — that the private sector may not be able to achieve. In that case a public-sector role may be necessary. These concerns are already reflected in legislative discussions at the state and federal levels. As those

discussions advance, it is useful to consider the questions that must be addressed if regulators are tasked with the additional responsibility to set data security standards and/or best practices.

By gathering together technologists, banking and payment industry representatives, merchants, and policymakers, we hope to further understanding of the complex economic and technological issues that are presented when considering a robust data security standard, one that can be adopted by most, if not all, payment system participants, from the smallest merchants and nonbanks to the largest payment networks, financial institutions, and payment processors.

This conference also aims to develop an appreciation for what these emerging technology solutions can and cannot do when it comes to protecting consumers' payment information. For example, in their current state, these technology solutions focus on enhancing data protection after customers have applied for and been approved as payment-card holders. They do not offer issuers a solution that can help at the time of application when authentication of new customers is a priority.

Finally, coordination on data security among these invited groups is imperative and is a necessary but not sufficient condition. This discussion is intended to provide insight on ways to improve collaboration on data security issues.



## Tuesday, February 16, 2010

- 4:00 p.m.      **Registration**
- 4:30 p.m.      **Keynote Address:** Professor Steven J. Murdoch, Computer Laboratory Security Group, University of Cambridge
- 5:15 p.m.      **Reception**
- 

## Wednesday, February 17, 2010

- 8:00 a.m.      **Registration and Continental Breakfast**
- 8:30 a.m.      **Opening Remarks:** Bob Hunt, Director, Payment Cards Center, Federal Reserve Bank of Philadelphia

### Technology Panels

The first three panels will address the following questions:

How do we define the technology? Which parties in the payment process would adopt it? What aspects of the payment process does it protect? Can we predict the effect of adopting this technology on levels of payment card fraud? What would be the remaining data security risks? Should this technology be combined with other solutions? What are the costs of implementing the technology? Is it sufficiently effective and affordable to be adopted widely? Are there any standard-setting issues to consider? Are there any impacts for consumers?

- 8:45 a.m.      **Tokenization**  
Moderator: Joonho Lee, Assistant Vice President, Federal Reserve Bank of New York  
Speakers: Rick Van Luvender, First Data Corporation  
Robert McMillon, RSA  
Hugh Njemanze, Arcsight  
Robert Vamosi, Javelin Strategy and Research
- 10:15 a.m.      **Break**
- 10:45 a.m.      **End-to-End Encryption**  
Moderator: Peter Burns, Senior Payments Advisor, Heartland Payment Systems  
Speakers: Bob Carr, Heartland Payment Systems  
Mike Herman, Chase Paymentech  
John Latimer, TSYS  
Eduardo Perez, Visa Inc.
- 12:15 p.m.      **Lunch**
- 1:15 p.m.      **Chip Technology**  
Moderator: Richard J. Sullivan, Senior Economist, Federal Reserve Bank of Kansas City  
Speakers: Simon Hurry, VISA Inc.  
Catherine Johnston, ACT Canada  
Sid Sidner, ACI Worldwide  
Randy Vanderhoof, Smart Card Alliance
- 2:45 p.m.      **Break**



3:15 p.m.

### **The Way Forward**

The final panel will have a Q&A format. A nonexclusive list of questions is listed below.

Moderator: Bruce Summers, Former Director, Federal Reserve Information Technology

Speakers: Cathy Allen, The Santa Fe Group

Hemant Bajjal, World Bank

Mike Cook, Wal-Mart

Bob Russo, PCI Council

### **Questions:**

When adopting a new data protection solution, what is required to establish an effective consensus among the diverse participants in consumer payments systems? How might coordination be improved and is there a role for government in facilitating such coordination?

Risk management priorities, and associated investments in technology, may be different for bank-card issuers, merchant acquirers, processors, and card-accepting merchants. Is the PCI-DSS process a mechanism that can be leveraged to balance incentives?

How might legislative or regulatory efforts help to better secure consumer payment systems? Is there an appropriate role for government in standard-setting or in supporting adoption of best practices? If so, under what circumstances?

Can we learn from other countries' experience in adopting these or other fraud prevention technologies? Can we or should we think about any lessons learned from data protection standards in other industries, e.g., health care (HIPAA)?

When considering technology solutions, are there hidden costs to consumers in terms of inconvenience and time demands? How might these costs affect adoption of technologies that make consumer payments more secure?

For more information, including events we sponsor and the research we produce, please visit our website.



FEDERAL RESERVE BANK OF PHILADELPHIA

Payment Cards Center

<http://www.philadelphiafed.org/payment-cards-center/>