SHADOW FINANCIAL REGULATORY COMMITTEE

COMMITTEE MEMBERS

GEORGE G. KAUFMAN
Co-Chair
Loyola University Chicago

RICHARD J. HERRING
Co-Chair
University of Pennsylvania

SHEILA BAIR
Pew Charitable Trusts

MARSHALL E. BLUME
University of Pennsylvania

KENNETH W. DAM
University of Chicago Law School and Brookings Institution

FRANKLIN EDWARDS
Columbia University

ROBERT A. EISENBEIS
Cumberland Advisors

EDWARD J. KANE
Boston College

PAUL KUPIEC
American Enterprise Institute

ALBERT S. KYLE
University of Maryland

KENNETH E. SCOTT
Stanford Law School

CHESTER SPATT
Carnegie Mellon University

PHILIP E. STRAHAN
Boston College

An independent committee sponsored by the American Enterprise Institute

http://www.aei.org/shadow

Administrative Office
c/o Professor George Kaufman
Loyola University Chicago
820 North Michigan Avenue
Chicago, Illinois 60611
Tel: (312) 915-7075
Fax: (312) 915-8508
E-mail: gkaufma@luc.edu

Statement No. 349

Kenneth W. Dam
(773) 255-2428

Robert A. Eisenbeis
(800) 257-7013

George G. Kaufman
(312) 915-7075

`

Statement of the Shadow Financial Regulatory Committee on

Data Breaches and Payment System Risks

February 10, 2014

The large data breaches at Target and a number of other retail merchants in recent weeks have been viewed in the media as principally a consumer protection concern. The Shadow Financial Regulatory Committee believes that the issues go far beyond the consumer and threatens the payments system as a whole. The recent data breaches raise numerous policy issues that extend far beyond this specific incident. There is the potential that Congress will rush to judgment and pass legislation to only expand consumer protections. But this is not sufficient because such breaches could wreak havoc with retail payments and also move through the payments processing chain. Vulnerable institutions include not just financial institutions but also retail firms and non-financial businesses that are electronically intertwined and potentially exploitable via the internet.

The potential for gigantic fraud losses has escalated sharply with the recent explosive growth of the internet, which now provides a potential window into the data of many millions of citizens' personal information. Remote internet access can enable anyone – even far removed from the United States – to obtain credit and other pertinent information and use that information to steal funds. Experience shows that when such information is compromised, consumers may rationally pull back and request cancellation or reissuance of existing cards, or resort to cash— essentially abandoning the payments system. Thus, hacker attacks can undermine the integrity of the payment medium and result in additional costs both to firms like Target and to the financial

institutions that must resolve the losses, sort out consumer identity problems, and reissue millions of cards.

There are many points of vulnerability to the payments system, especially since many institutions have outsourced the actual processing and warehousing of data. This trend in outsourcing is accelerating as more and more businesses move their computing into the cloud, which may or may not embody adequate data encryption procedures. While banks at the end of the payments chain may have very sophisticated methods to identify fraudulent transactions, there are still many points of entry outside of commercial banks through which potential damage can be done. A recent Verizon Business Solutions survey points out that less than 11% of non-financial firms have installed protections that meet minimum industry standards that industry cyber security experts assert are not now sufficient given current hacker technology.

The overarching issues concern risks to the payment system itself and the threat that breached information will be used to commit wholesale electronic theft. This can threaten the solvency of a major financial institution, such as a bank, an investment bank, an insurance company, or a major non-financial firms whose demise could have huge real side ripple effects to the economy. The risks are further amplified by the complex interrelationships among non-financial business firms, operators of the private-sector payments-transfer infrastructure, and financial firms. If confidence in electronic payments systems can't be trusted, large efficiency losses would result.

Given the magnitude of the damage that data breaches could inflict on the US financial infrastructure, what should be done? Because of the potential for systemic risk, the Shadow Financial Regulatory Committee concludes that the issues should be addressed and given a high priority by policy makers including, perhaps, the Financial Stability Oversight Council (FSOC). Policy makers need to identify the potential risks, recommend improvements in security measures that financial and nonfinancial firms should make, propose loss-sharing rules to eliminate uncertainty and costly litigation, review and make recommendations to modernize federal rules concerning debt and credit protocols, and consider what efforts should be undertaken internationally to curb unscrupulous use of the internet.