NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Chairman

FOR IMMEDIATE RELEASE

Statement of Chairman Bennie G. Thompson

Do the Payment Card Industry Data Standards Reduce Cybercrime?

March 31, 2009 (Washington) – Today, Committee on Homeland Security Chairman Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Emerging Threats, Cybersecurity and Science and Technology Subcommittee hearing entitled "Do the Payment Card Industry Data Standards Reduce Cybercrime?":

"From our personal computers to our government networks to our critical infrastructure, the United States and its citizenry are under attack in cyberspace. The adversary ranges in skill, from unsophisticated to highly capable, from lone hackers to organized crime and nation states. Their intent ranges from nuisance and disruption to theft, espionage, and warfare. Their successes are varied – for every hacker that we have caught and prosecuted, thousands continue to work unabated. In December 2008, the Center for Strategic and International Studies concluded that the battle for cyberspace is one that we are not winning.

Willie Sutton was rumored to have said he robbed banks "because that's where the money is." In today's world of payment card transactions, the money is now located on computer networks. On any given day, billions of dollars flow back and forth between merchant and payment card networks, which process credit card numbers for transactions. It is an area that is ripe for hackers to exploit, and they are taking advantage of weaknesses in the system.

Experts suggest that in this "invisible war," it is difficult to estimate how much money is lost to cybercrime each year. According to the 2008 Internet Crime Report, the Internet Crime Complaint Center received over 275,000 complaints of crimes perpetrated over the Internet, a 33 percent increase from the previous year. The complaints received amounted to nearly $265 million in reported losses. Credit and debit card fraud amounted to around 5 percent of this total loss. This report does not represent all victims of Internet crime or fraud because it is derived solely from information provided by the people who filed a complaint with IC3. According to a 2009 report from McAfee, the 2008 overall losses from data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage last year. Respondents estimated that they lost data worth a total of $4.6 billion and spent about $600 million cleaning up after breaches.

Though the numbers vary, one thing is clear: securing our computers and the information contained within our information infrastructure is a serious national and economic security issue that we ignore at our own peril. Any money or information that we lose to malicious actors could potentially be used against this country and its citizens. That is why we must be diligent in reducing massive data breaches, and that is why this Committee will continue to pursue its investigation into cybercrime and terrorism funding.

We are here today to learn about the private sector efforts to combat data breaches and cybercrime, and to assess the quality of the Payment Card Industry Data Security Standards. The Standards have been around for several years, but massive, ongoing data breaches at some of America's largest merchants suggests that the Standards are inadequate to prevent breaches. The essential flaw with the PCI Standards is that it allows companies to check boxes, but not necessarily be secure. Checking boxes makes it easier to assess compliance with a Standard. But compliance does not equal security.

We have to get beyond check box security. It provides a false sense of security for everyone involved, and it is ineffective in reducing the real threats. Companies need to understand that

even if 100 percent compliance with the PCI Standards is achieved, hackers will continue to develop techniques to exploit the computer systems of companies holding cardholder data. You are not safe unless you continually test your systems.

Today, we are calling for change. I call on the payment card industry and the thousands of merchants and vendors who have to comply with the standards to rededicate themselves to the goal of securing their networks. For the payment card industry and the issuing banks, this is going to mean significant investment in infrastructure upgrades. As the Chair has pointed out, these investments are already occurring overseas. I am puzzled and disappointed that we are not seeing similar upgrades here domestically, and I hope our witnesses can explain why the card industry appears not to be moving quickly to address these issues.

I am deeply troubled by the testimony that suggests credit card companies are less interested in substantially improving their product and procedures than they are with reallocating their fraud costs. The payment card industry's effort to shift risk appears to have contributed to our current state of insecurity, and I am concerned that as long as the card industry is writing the Standards, we will never see a more secure system. We in Congress must seriously consider whether we can continue to rely on industry created and enforced standards, particularly if they are inadequate to address ongoing threats. I look forward to working with my colleagues on both sides of the aisle and across Committee lines to further explore whether government action is necessary to protect against these threats. One thing is certain: the current system is not working."

# # #

FOR MORE INFORMATION: Please contact Dena Graziano or Adam Comis at (202) 225-9978

United States House of Representatives
Committee on Homeland Security
H2-176, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
http://homeland.house.gov