EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE
RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900
www.house.gov/markey

June 22, 2005

The Honorable Michael Chertoff
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

The Honorable Robert S. Mueller III
Director
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Secretary Chertoff and Director Mueller:

Last week's announcement that hackers infiltrated CardSystems Solutions, resulting in what has been described as the largest data theft in history, once again raises serious concerns about the security of consumers' personal information that is maintained, stored, and transported for commercial purposes beyond the control of consumers. I am also concerned, however, that the recent wave of information thefts which has swept up the personal information of millions of Americans over the past several months not only may harm the consumers whose data were stolen, but also may have serious homeland security implications for our country. Indeed, Dennis Lormel, the former chief of the FBI's terrorist financial review group, previously identified the connection between data breaches, identity fraud and terrorism, stating that "I don't think people have really gotten the message. We have known terrorists out there who are exploiting identity theft and identity fraud vulnerabilities."[1] I am writing to request that the Department and the Bureau examine this spate of security breaches with an eye towards whether any may represent attempts by terrorist organizations to fund their activities through the theft and sale of consumers' personally identifiable information.

In addition to the theft at CardSystems Solutions announced last Friday, ABC News reports that there have been over 40 major reports of data theft and loss in the last three years. These cases have involved such prominent companies as Time Warner, Ameritrade, and DSW Shoe Warehouse. Data theft affects an increasingly large number of Americans with each new case. A 2003 FTC survey showed that over a one year period nearly 10 million people – 4.6% of the adult population – had discovered that they were victims of some form of identity theft.

As you know, data have been stolen via electronic breaches and lost during physical transport of tapes. On February 25, 2005, Bank of America announced it had lost computer backup tapes containing personal information such as names and Social Security numbers on about 1.2 million federal-government charge cards. Among those affected by this loss were roughly 900,000 employees of the Defense Department and about 50 U.S. Senators. These tapes disappeared during a truck delivery route to the storage facility. The tapes were

[1] *No Place to Hide*, Robert O'Harrow, Jr, 89.

unencrypted, allowing for easy access to the stored personal information. According to *USA Today*, only 6% of financial service companies and 7% of businesses encrypt their backup tapes. A similar incident involving the physical transportation of backup tapes to a storage facility involving Time Warner occurred on May 2. These tapes contained personal information of over 600,000 current and past employees.

Eleven of the largest cases of identity theft in 2005 have affected roughly 8 million U.S. citizens so far this year. These cases involve a wide variety of companies, from Polo Ralph Lauren, to ChoicePoint, to Ameritrade. In his recent book *No Place to Hide*, Robert O'Harrow, Jr. included a quote from the director of the Center for the Study of Terrorism and Political Violence at the University of St. Andrews, who told *Newsweek* in 2002 that "Identity theft – credit card theft, bank fraud – is hugely important to al Qaeda, as it is to many terror groups. I've been astonished that there has been so little attention to it."[2]

I am interested in the Department's and the Bureau's views on the potential effects of these breaches on our nation's homeland security and would appreciate responses to the following questions:

1. Please examine these cases, and others that may have come to the Department's or Bureau's attention, and indicate whether they represent a potential terrorist opportunity that could threaten the security of the United States or our allies. If the Department or Bureau is concerned about this possibility, please indicate whether any of these breaches looks particularly problematic, either based on your concern that a breach appears to be a deliberate attempt to fund terrorist activities through identity theft, or that a breach appears to an opportunity for terrorists to exploit a breach even if they were not the cause of it.

2. As you know, the recent cases of missing identity information involving companies such as Time Warner, Ameritrade, Citigroup, and Bank of America have involved the physical transfer of this information on non-encrypted backup tapes. Does the Department or the Bureau view the failure of companies to encrypt such data as a risk that could have implications for our country's homeland security if the data were stolen by terrorist groups? If yes, would the Department or the Bureau support legislation to require encryption of vital personally identifiable information stored by data brokers, financial information and other commercial entities? If not, why not?

3. Four prominent cases of data theft have involved the disappearance of the backup tapes during truck delivery routes.[3] In these instances is the Department or the Bureau aware of whether the drivers had any criminal background or links to terrorist activities or organizations? In these cases, has the Department or the Bureau investigated the existence of such potential links?

4. One of the most recent cases of the loss of personal information involved the theft of data belonging to Federal employees. How many cases between March 1, 2003 and June 1, 2005 have involved federal employees, including military personnel? Does the Department or the Bureau believe that cases in which the personal information of federal employees is stolen presents a greater homeland security risk than a case that does not result in the theft of such information? If yes, please explain why. If not, why not?

5. What is the Department's or the Bureau's role in the investigation of identity theft cases? *The Wall Street Journal* has indicated that the Secret Service is involved in several recent cases of identity theft.[4] How specifically is the Secret Service involved in these cases, and which other entities within the Department are responsible for investigation of identity theft? How may staff members within the Department and the Bureau

---

[2] *Ibid.*, 90.
[3] "Without a Trace", *Wall Street Journal,* June 17, 2005.
[4] "Time Warner Alerts Staff to Lost Data", *Wall Street Journal, May 3, 2005*

are responsible for investigation of links between identity thefts and terrorist activities? Between March 1, 2003 and June 1, 2005, how many identity theft cases have been resulted in criminal prosecutions? How many have resulted in convictions? Of these cases, how many of the individuals involved have had ties to terrorist organizations or activities?

6. Does the Department or the Bureau believe that terrorists are unable to purchase information collected by data brokers such as ChoicePoint to support their own terrorists activities? If yes, what evidence does the Department or the Bureau have to support this assertion? If not, what are the Department and the Bureau doing to deny terrorists access to such valuable information?

7. According to NBC 10, a Southern New England television station, last year the Department distributed a form in public schools to be carried by students for use in emergencies.[5] Along with the name, address, and emergency phone number of the student, the form also included a section to write the Social Security number. With the growing improper use of Social Security numbers to perpetrate fraud, is it advisable for the Department to encourage students to provide such information, particularly in light of the recent instance in which a professor at a community college in Winter Haven, FL directed students to furnish their Social Security numbers on attendance sheets, which he then used to fraudulently obtain credit cards in the names of his students?[6] In the Department's and the Bureau's view, should measures be taken to reduce the role and frequency of Social Security numbers in commercial transactions? As you may know, I have introduced legislation, H.R.1078, the Social Security Number Protection Act, to prohibit the sale or purchase of Social Security numbers? Does the Department or the Bureau consider such efforts to limit to legitimate purposes the availability of Social Security numbers to be a beneficial policy from a homeland security standpoint?

Thank you in advance for providing responses to these questions. If you have any questions about this inquiry, please have a member of your staff contact Mr. Mark Bayer or Mr. Jeff Duncan of my staff at 202-225-2836.

Sincerely,

Edward Markey

[5] A copy of this form is posted on the DHS Web site Ready.gov: http://www.ready.gov/pdf_familycommunications.html?id=fcp

[6] "Professor Accused Of Stealing IDs Of PCC Students", *Tampa Tribune*, June 6, 2005.