



One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515
March 3, 2005

The Honorable David Walker
Comptroller General
Government Accountability Office
Washington, DC

Dear Mr. Walker:

Recently, ChoicePoint made public that criminals gained access to its massive database of private consumer information. We are concerned that this and similar breaches could be used by terrorist organizations to steal identities and credit information. Terrorists could use this information to enter the United States illegally or to finance terrorist attacks. We request that the Government Accountability Office review this matter further.

ChoicePoint's database has 19 billion public records that include everything from motor vehicle registrations, license and deed transfers, military records, names, addresses and Social Security numbers. Thieves were able to access this information, according to public reports, and make hundreds of thousands of U.S. consumers vulnerable to identity theft.

This security gap places America at risk. There is nothing to stop an organized terrorist organization like Al Qaeda from using this vulnerability to access the personal information of private citizens and use it against our nation. With the information that companies like ChoicePoint maintain, terrorists could have a better chance of entering the United States, they could better smuggle finances, and could obtain better cover when preparing to perform terrorist attacks. As noted in a February 21 *USA Today* article, "cyberfraud, ranging from credit card theft to money laundering is the latest wrinkle in terrorists' use of the Internet."

In order to better understand what the Department of Homeland Security and other national security agencies are doing to ensure that commercial databases containing private information are secure, we ask that you:

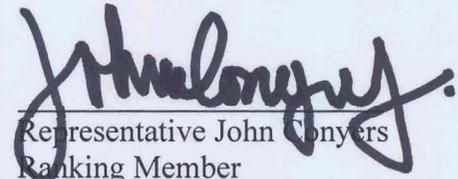
1. Provide us with a briefing on what the Department is specifically doing to advise ChoicePoint and similar commercial database aggregators on how to protect personal information contained in their systems;
2. Work with the private sector to determine what further steps must be made to secure these large databases from terrorist attack; and
3. Explain whether the Department is working with other agencies to determine how to prevent and respond to future attacks. Please include in this response any information on whether the Department or other agencies had worked, prior to the ChoicePoint attack, on securing commercial databases containing personal information.

We look forward to a detailed response from you within 30 days that addresses the opportunities ChoicePoint and similar databases provide to terrorists.

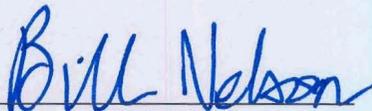
Sincerely,



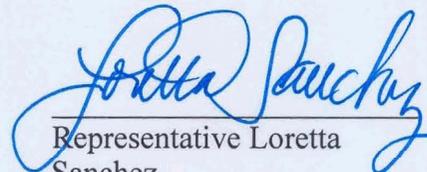
Representative Bennie G. Thompson
Ranking Member
House Committee on Homeland Security



Representative John Conyers
Ranking Member
House Judiciary Committee



Senator Bill Nelson
Ranking Member
Subcommittee on International Operations
and Terrorism,
Senate Foreign Relations Committee



Representative Loretta
Sanchez
Ranking Member
Subcommittee on
Economic Security,
Infrastructure Protection, and
Cybersecurity,
House Committee on
Homeland Security



Representative Zoe Lofgren
Ranking Member
Subcommittee on Intelligence, Information Sharing,
and Terrorism Assessment,
House Committee on Homeland Security