



For Immediate Release  
August 5, 2008

Contact: Dan Virkstis  
(202) 224-4515

## BAUCUS CHALLENGES “TEPID” IRS RESPONSE TO I.D. THEFT

*Finance Chairman calls for more action, details on strategy to combat identity fraud*

**Washington, DC** – Senate Finance Committee Chairman Max Baucus (D-Mont.) commented today on an Internal Revenue Service (IRS) update and accompanying letter on its Identity Protection Strategy, the details of which were requested by Senator Baucus at an April Finance hearing. The report demonstrates some improvement to IRS processes, most notably that taxpayers will be able to “self-report” to the IRS when their identities have been stolen, rather than having to wait and see if their information will be fraudulently used by another person to file a tax return. However, Baucus expressed concern that the response he received from the IRS does not constitute an earnest attempt to address the issue of identity theft. The Senate Committee on Finance has jurisdiction over U.S. tax policy, including oversight of the IRS.

**“Identity theft is a growing and serious issue that victimizes too many Americans. And while this report is full of good intentions, its actual treatment of the problem is tepid and insufficient,”** said Baucus. **“I need the IRS to give me clear, substantive answers on their strategic plan – and its implementation – to treat and resolve cases of identity theft. I intend to follow up with Commissioner Shulman to make certain that my expectations are clear.”**

Specifically, Baucus intends to get clarity on the overall design of the IRS identity theft strategy with attention to specific goals, measures and timelines; to find out how soon the agency will be able to prevent recurring holds on taxpayer accounts in cases of identity theft; to determine whether there will be a central point of accountability at the IRS; to know if the IRS will contact taxpayers when someone files using their social security number; to learn the extent to which the IRS will use Federal Trade Commission (FTC) data to determine or confirm identity theft; and the extent to which IRS procedures to avoid identity theft affect the ability of the IRS to operate efficiently.

The text of the letter and IRS report follow here:

July 21, 2008

The Honorable Max Baucus  
Chairman  
Committee on Senate Finance  
United States Senate  
Washington, DC 20510

Dear Mr. Chairman:

Thank you for the opportunity to present an update on the Internal Revenue Service's (IRS) Identity Protection Strategy. Identity theft exacts a heavy financial and emotional toll on its victims and increasingly burdens our economy. Because the IRS touches almost all Americans, a comprehensive approach is needed to assist taxpayers who are identity-theft victims and to combat vigorously the effects of this crime. When a taxpayer contacts us with an issue or concern, we should have in place a seamless process that gets the issue resolved promptly. From the perspective of an identity-theft victim, that means the taxpayer can reach someone at the IRS who is knowledgeable on the issue and who is able to take care of the problem quickly and permanently.

The IRS is focused on prevention and assistance activities including a comprehensive approach to protecting taxpayer information. As is discussed in the attached strategy, the IRS will enhance efforts through three overarching goals: Victim Assistance, Outreach, and Prevention.

When identity-theft victims seek assistance from a government agency, they have the right to expect the agency to help them -not add to their problems. The IRS will continue to work diligently to reduce the burden placed on the taxpayer and the tax system as a result of identity theft.

Sincerely,

Douglas H. Shulman

### **Identity Theft and Tax Administration Implications**

Assisting taxpayers in efforts to prevent and respond to the tax implications of identity theft continues to be a major priority of the Internal Revenue Service (IRS). Identity theft can cause undue harm to taxpayers by negatively affecting their tax account in one of two ways. First, a taxpayer's identity could be used by a criminal to obtain a fraudulent tax refund. Second, a criminal could use the stolen information to obtain employment. In either case, the true taxpayer may be unaware that his or her identity has been compromised.

### **Victim Assistance: Assist taxpayers with resolving tax issues associated with identity theft**

The IRS is committed to providing services to help identity-theft victims resolve tax issues as quickly as possible and with minimal taxpayer disruption. We will continue to refine these services to reduce undue taxpayer burden and to meet the unique needs of identity theft victims consistently.

This January, the IRS began tracking identity-theft cases using an indicator to mark the taxpayer's account once identity theft has occurred. Beginning in January 2009, we will use this indicator to distinguish legitimate returns more easily from fraudulent returns submitted by identity thieves. In October 2008, we will also offer taxpayers the opportunity to self report incidents of identity theft that occur outside of tax administration. These new processes support victims by requiring them to submit documentation validating the identity theft only once. In addition, these indicators enable all IRS functions to identify affected accounts quickly and to monitor them throughout the resolution process. These efforts will reduce taxpayer burden by expediting the process for

identifying potential victims and successfully resolving their current tax issues. In addition, the indicator may help prevent future tax issues.

The IRS is currently working to provide taxpayers with a central point of contact for the resolution of tax issues caused by identity theft. Beginning in October 2008, we will open a specialized identity-theft victim assistance center that will be fully dedicated to resolving tax issues incurred by identity theft victims. This service will enable victims to have their questions answered and issues resolve quickly and effectively.

We are developing a process to contact taxpayers quickly when the IRS has evidence that the taxpayer's personal information may have been compromised. As we verify the helpfulness of these communications, we will enhance them to provide these taxpayers with relevant information regarding their account and the incident that has occurred. This information is vital to taxpayers who may not be aware that their identity has been stolen. In addition, the IRS will ensure that taxpayers have access to the information and resources they need to resolve tax issues caused by identity theft.

### **Outreach: Increase taxpayer awareness of identity theft**

The IRS will continue to provide taxpayers with information to increase their awareness of identity theft and to resolve related tax issues. When expanding outreach activities, the IRS considers the diverse needs of taxpayers and will work with partners to meet the unique needs of identity theft victims.

The IRS will continue to recommend methods for keeping taxpayers' personal information safe and out of the reach of identity thieves. To satisfy the diverse needs of the taxpayer population, we will use a wide variety of channels to communicate with the public. During the recent filing season, we created a link on the homepage of IRS.gov to direct taxpayers to the latest information on new phishing schemes. In addition, we frequently update a specialized webpage on IRS.gov to share information with taxpayers on emerging trends, phishing sites, schemes, and prevention strategies. This site enables taxpayers to obtain quickly and easily the information necessary to answer their most common questions.

The IRS is also directing victims to the most up-to-date identity-theft information to ensure that they know how to report identity-theft crimes and have the necessary resources and support to recover their identity. In April 2008, in addition to helping taxpayers resolve any tax issues, we began referring them to the FTC's consumer education site, OnGuardOnline.com, to provide additional guidance on protecting personal information and avoiding Internet fraud.

The IRS will continue to collaborate with industry leaders, tax professionals, and other federal agencies, including the Social Security Administration, the FTC and the Department of Homeland Security, to gather information on emerging issues related to identity theft. For example, the IRS is hosting an Identity Protection Forum in July 2008 where industry leaders will meet to discuss the effects of identity theft on its victims and best practices for prevention and resolution. By collecting and analyzing data from multiple sources, the IRS will ensure that it is up to date on identity-theft trends and uses this knowledge to enhance existing processes.

### **Prevention: Build programs to reduce incidents of identity theft and protect the American taxpayer**

The IRS protects taxpayers by continually enhancing efforts to safeguard personal information and by working to detect online identity-theft fraud schemes before they affect taxpayers. Criminals from within the United States and from foreign countries create fraudulent internet sites purporting to be the IRS or one of our agents. These sites are used to gather personal identity information including SSNs, income, date of birth, and bank accounts from their victims. Last year, we implemented a program to address the increasing and evolving threat of online identity theft affecting the IRS and taxpayers.

The IRS has formed a group of highly trained security specialists to detect suspicious online sites, to analyze the sites' content and source, and to ensure that fraudulent sites are shut down. Since last October, this group has identified and shut down over 2,000 fraudulent sites from all over the world. The group has developed a rapid response capability and the average time from fraudulent site detection to site shut down is 10 hours. This rapid response minimizes the number of identity-theft victims.

Perpetrators of online fraud frequently create multiple bogus websites. Often, as soon as one fraudulent site is shut down, another is brought on-line. Therefore, it is important to track down these criminals quickly. We work with law enforcement agencies, including the Department of Justice (DOJ) and the Treasury Inspector General for Tax Administration to pursue criminal investigations. These efforts include gathering evidence, issuing search warrants, and, if appropriate, filing charges against perpetrators of online fraud.

Because online fraud is an evolving crime, it is important that we work with other governmental agencies and the private sector to share information and to stay current on the latest trends. We strengthen our national response to online fraud by cooperating with the U.S. Secret Service Electronic Crimes Task Force, the DOJ Computer Crime & Intellectual Property Section, and the FTC. In addition, we partner with the public sector to learn of trends and to raise awareness of this problem. We also participate with outside organizations such as the National Cyber Security Alliance Anti-Phishing Task Force and the Multi-State Information Sharing and Analysis Center, which are dedicated to stopping online fraud. By expanding our prevention efforts, we are reducing the potential risks to personal information and the occurrence of tax issues related to identity theft.

The IRS will continue to provide comprehensive identity-theft education programs and supporting tools to all employees to expand their knowledge of identity-theft issues and efforts to safeguard personal information. For example, an internal website has been developed to provide current information to IRS employees on issues related to data protection techniques. This spring, all IRS employees received training on standard procedures for encrypting data and using identity information.

In the future, we will continue to train employees on emerging identity-theft issues encountered by victims. The IRS will also make tools available to employees to support their efforts to resolve tax issues of identity theft victims. For example, we are developing a centralized manual that will include information on identity-theft case processes and procedures and that will be regularly updated with the most current information. This will enable IRS employees to find the information in a central location to resolve-identity theft cases consistently and effectively and respond to frequently asked questions.

Additionally, the IRS is working to reduce the unnecessary use of Social Security numbers (SSNs) in communications with taxpayers and in internal documents and systems where an

employee identifier is required. An SSN can be a valuable piece of information for an identity thief because it is often used to verify an individual's identity. In many cases, a unique identifier other than an SSN can be used in documentation related to individual taxpayers or employees. By reducing the use of SSNs, the IRS is significantly lowering the risk of this information being used to commit a crime.

###