

Committee on Ways and Means
Subcommittee on Social Security
Joint Hearing with Committee on Financial Services'
Subcommittee on Oversight and Investigations on
Preventing Identity Theft by Terrorists and Criminals
Opening Statement of Chairman Shaw
November 8, 2001

Today, our two Subcommittees join together to examine ways to prevent identity theft by terrorists and criminals.

When Social Security numbers were created 65 years ago, their only purpose was to track a worker's earnings so that Social Security benefits could be calculated. But today, use of the Social Security number is pervasive.

Our culture is hooked on Social Security numbers. Businesses and governments use the number as their primary source of identifying individuals. You can't even conduct the most frivolous transaction --like renting a video at your local store -- without someone asking you to first render your 9 digit ID.

Your Social Security number is the key that unlocks the door to your identity for any unscrupulous individual who gains access to it. Once the door is unlocked, the criminal or terrorist has at their fingertips all the essential elements needed to carry out whatever dastardly act they can conceive.

We now know that some terrorists involved in the September 11th attacks illegally obtained Social Security numbers and used them to steal identities and obtain false documents, thus hiding their true identities and motives. These unspeakable acts shine an intense spotlight on the need for government and private industry to be vigilant in protecting identities. It also demands that safeguards to prevent identity theft are put in place now.

Earlier this year, I along with several of my Ways and Means colleagues, introduced H.R. 2036, the "Social Security Number Privacy and Identity Theft Prevention Act of 2001."

This bipartisan bill represents a balanced approach to protecting the privacy of Social Security numbers while allowing for their legitimate uses. Because of its broad scope, the bill has been referred to the Committee on Energy and Commerce and Committee on Financial Services, in addition to Ways and Means. I urge prompt action by all three committees so we may bring this important legislation to the floor as quickly

as possible. It is a needed part of our nation's response to terrorism.

Sadly identity theft is a crime not perpetrated just against the living. A *Washington Post* article on Saturday, September 29, reported that a man detained in Great Britain, and suspected of training four of the terrorists who hijacked the airliners on September 11, used the Social Security number of a New Jersey woman who died in 1991. The Associated Press reported on October 31 that an individual from North Carolina had been indicted on charges he tried to steal the identity of someone killed in the terrorist attack at the World Trade Center.

Therefore today, we will take a hard look at the sharing of death information. The Social Security Administration maintains the most comprehensive file of death information in the federal government. How this information is compiled, its accuracy, and the speed with which it is shared with the public will be explored.

Because the financial services industry relies fundamentally on Social Security numbers as the common identifier to assemble accurate financial information, they are in a unique position to assist in the prevention of Social Security number fraud and abuse. Their timely receipt of death information and prompt updating of financial data is key in preventing identity theft.

In the past, some businesses have not been "enthusiastic" about further restricting the use of Social Security numbers. It is my hope they will rethink their resistance in light of September 11. Identity theft is a national security threat involving life and property. Safeguards will be made and I predict sooner, rather than later.