

Comments to the Federal Trade Commission
The Role of Social Security Numbers as Authenticators
September, 2007

The FTC asks for comments regarding the use of SSNs as authenticators, and specifically seeks comment on the costs and challenges of eliminating the use of SSNs as authenticators.

Many businesses and other institutions continue to use SSNs as unique personal identifiers. That, by itself, is not necessarily a problem. But partly because of this widespread use of SSNs as unique numerical identifiers of individuals, a given SSN cannot be considered to be “secret” information known only to the rightful “owner” of that number. The problem comes when businesses and other institutions then treat these numbers as authenticators, meaning that they regard the mere knowledge of a particular SSN as “proof” that someone who claims the identity of a person associated with a particular SSN is truly that person. Many times it is not even necessary to know the whole SSN. It’s not uncommon to be asked for “the last 4 digits of your Social” when dealing with some business with which we have a relationship, as “proof” of our identity.

Because of this practice of using SSNs as authenticators, knowledge of someone else’s SSN is a great enabler of identity theft. It’s not difficult to get a new credit card online, for instance, by providing a SSN in combination with other personal information. The credit grantor checks the credit score associated with the SSN provided, and if it is good enough, a new credit account is then associated with the SSN. This, despite the fact that the personal information and SSN used to open the account may not pertain to the person using it to open the account.

Congress has become aware of identity theft, and usually proposes three types of “fixes” to deal with the problem: stronger penalties for identity theft, stronger information breach notification laws, and proposals to restrict the use of SSNs. Lately, a fourth solution has been proposed: a “security freeze” that people can place on their credit files, to prevent credit information from being accessible by a credit grantor who might open a new account for an identity thief. While these are all good and worthwhile measures, only the security freeze laws seek to make a stolen SSN less useful for opening a new account using someone else’s identity. The problem is simply that our personal information resides in many databases, as well as in paper form, in many different places. Any approach that seeks to prevent others from using our identity by attempting to somehow make identity information “secret” again is bound to fail in the long run. There simply needs to be a better way to authenticate someone’s claim to a particular identity that does not rely solely on knowledge of personal information, including a SSN.

Although it’s possible to address this problem in more than one way, here is one suggestion. The suggestion ties in with the fact that credit grantors typically will check with a credit bureau to determine whether someone is credit-worthy before establishing a new account for that person. As part of that credit check, suppose an identity check could also be provided. This could be implemented as an opt-in service that would require

interested individuals to “register” their identities (ie, their SSNs) on a kind of “Call Me First” list, patterned along the lines of the ever-popular Do Not Call list. A person who can prove that they “own” a particular SSN would provide contact information to enable the credit bureau to contact them whenever someone attempts to use their SSN to establish a new credit account. When a particular individual is contacted by a credit bureau because his/her SSN and other identity-related information is being used to open an account, the individual would either grant or withhold permission for the credit bureau to provide credit-related information to the would-be creditor. If permission is withheld, not only would the credit bureau not provide the requested credit information, but the credit bureau could also notify the credit grantor that the “true owner” of the SSN being used in the credit application has specifically withheld approval for the information to be provided. This should send a warning signal to the credit grantor that the credit application is likely to be fraudulent.

A system such as this would seem to provide all the benefits of a security freeze, while eliminating many of the disadvantages. While the security freeze is somewhat of a blunt instrument against identity theft, in that it prevents *any* credit information from being provided unless the freeze is lifted, the Call Me First concept can give individuals more control over the dissemination of their credit information. No longer would it first be necessary to “unfreeze” your credit file at each of the three credit bureaus, and then “refreeze” it later on. Although the Call Me First concept is similar to a fraud alert, in that an individual is contacted to gain approval before an account is opened, it may be beneficial to depend on a very small number of credit bureaus to authenticate a new credit account, rather than depending on a much larger number of potential credit grantors to do it. One possible advantage is that it may be easier for the major credit bureaus to enforce some standards or best-practices for authenticating individuals, rather than assume that every credit grantor will follow such guidelines.

Of course, the “devil is in the details”, and the details of how such a proposal would be implemented must be worked out. But in addition to the availability of a Call Me First type of service, or any other proposal for better identity authentication that eliminates reliance on SSNs as authenticators, such capabilities need to be widely adopted and used by people in order to be effective against identity theft. This may be one area that the Federal Trade Commission might be able to play an active role. The government and other groups have long waged an effective campaign in the national media against drunk driving. Perhaps widespread adoption of better identity theft prevention measures, whatever they may be, may also require entities such as the FTC to wage similar advertising campaigns.

Bob Pinheiro

Robert Pinheiro Consulting LLC
bp@bobpinheiro.com
www.bobpinheiro.com