

## **Response to President's Identity Theft Task Force**

### **II. Preventing The Misuse of Consumer Data**

I'm responding to the Task Force's request for comments on how to prevent the misuse of consumer data that has fallen into the hands of an identity thief. As the Task Force noted in the Interim Recommendations to the President, "developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individual's information." I agree, and would point out that there is a key difference between authentication for preventing unauthorized access to existing accounts, and authentication for preventing identity thieves from opening new accounts in someone else's name. In the case of authentication for access to existing accounts, there is already an established relationship between the Relying Party (ie, the business where the account has been opened), and an account holder. Therefore, the Relying Party has previously provided the account holder with some type of authentication credentials for account access, even if those credentials are weak and can easily be compromised. In other words, the Relying Party does have some means for authentication of someone seeking access to an existing account, even if the authentication is based solely on knowledge of a password, which can be compromised in numerous ways. In the case of someone seeking to establish a new credit account with some business entity, however, often there is no previous relationship between the business entity and the person whose identity is being used to open the account. Therefore, the business entity has no direct means to authenticate the claimed identity of the person seeking to open the new account.

When someone unknown to a business entity seeks to establish a new account in-person, of course, the business can request to see a government-issued photo ID. The risk to the business entity is that the photo ID could be a fake, or that an imposter somehow managed to get a photo ID using someone else's identity information. But when someone seeks to establish a new account online, or over the phone, the business entity really does not have a good way to verify that the person seeking to open the new account is truly who they claim to be. The best that can be done today, if the business entity is sufficiently motivated to do so, is to ask "out-of-wallet" questions that only the actual person whose identity information is being provided could be expected to answer. However, this "knowledge-based" approach to authentication requires that the Relying Party entity subscribe to some commercial database service that gathers and sells personal information for various purposes, including identity verification. In most cases, this approach is not taken because of the cost and inconvenience. It may be employed if the Relying Party has some reason to be suspicious, but otherwise it is uncommon.

Although knowledge-based authentication is not widely used, it is likely that the business entity may check the credit rating associated with the identity being used to open the account. If the personal information provided, which usually will include a Social Security Number, matches at least some of the information in the credit file, there is an assumption that the person applying for the new account, and presenting the information, is truly the person whose identity information is being presented. In the case of identity theft, this information is stolen, so the assumption is false.

What is needed is a better way to authenticate the claimed identity of someone who is unknown to a business entity, and who presents personal identity information for the purpose of opening a new credit account online, or over the phone. I would propose that the Task Force should:

1. Hold a series of workshops that specifically encourage participants to propose better forms of identity authentication for the prevention of identity theft. The announcement of such workshops should be widely disseminated, to encourage not only academics and established businesses to participate, but also smaller businesses and other entrepreneurs and consultants.
2. Secure funding from the federal government to support research towards the development of better means of identity authentication specifically for identity theft prevention.
3. Ensure that the funding is open to small businesses, entrepreneurs, and consultants, possibly via grants made by the Small Business Innovation Research program of the Small Business Administration.
4. Explore ways to encourage the business community to actually make use of better authentication methods that may be developed for identity theft prevention. Unless better authentication methods are actually put to use, they will have no impact on preventing identity theft. Too often, businesses are willing to accept a certain amount of fraud as part of the cost of doing business. When it comes to identity theft, real people can be harmed beyond the financial losses that may be suffered by businesses. The government should devise incentives for encouraging the business community to actually adopt better authentication methods for identity theft prevention, as they become available.

Bob Pinheiro

---

Robert Pinheiro Consulting LLC  
[www.bobpinheiro.com](http://www.bobpinheiro.com)