



January 18, 2007

Identity Theft Task Force, P065410  
Federal Trade Commission  
Office of the Secretary, Room H-135 (Annex N)  
600 Pennsylvania Avenue, NW  
Washington DC, 20580

Dear Members of the White House Identity Theft Task Force:

ID Analytics appreciates the opportunity to submit comments to the Task Force as it develops a strategic plan to combat identity theft. This document discusses four key recommendations that, based on our experience, will significantly improve the effectiveness of federal government efforts to reduce identity theft:

1. More concrete research is needed to define the scope of identity theft;
2. Data breach notification standards should be linked to harm;
3. Government entities should focus on improved methods of authentication;
4. Regulation should allow the private sector to innovate and collaborate.

**MORE EMPIRICAL, SCIENTIFIC RESEARCH NEEDED:**

We strongly recommend that Federal agencies conduct or sponsor additional empirical research on identity theft. We make this recommendation out of concern that the current understanding of the amount, cost, and sources of identity theft has significant gaps. Too little is known about the incidence of the actual crime, the channels through which the crime is committed, as well as emerging fraud trends. Even where research is available, findings are often widely varying.

It is noteworthy that many commonly cited studies rely on surveys of small populations in which the incidence of identity theft is self-reported by consumers. These types of surveys have significant constraints. First, it is quite common for identity theft victims not to know how fraudsters gained access to their personal information. Secondly, consumer confusion over the definition of identity theft can lead to errors in self-reporting. Consumers also can only report identity theft if they are aware of the crime and, in some cases, it may take years for individuals to learn they are victims.



Better insight into the mechanics of identity theft is critical to effective solutions and policy making in this area. An effective legislative response, for example, to recent data breaches depends on an accurate assessment of the level of identity theft emerging from breaches. Organizations have a finite amount of resources to combat identity theft. The most efficient way to deploy these resources is against the actual incidence and risk of identity theft.

### **DATA BREACH NOTIFICATION STANDARDS SHOULD BE LINKED TO HARM:**

We recommend that data breach notification standards should reflect the likelihood of harm resulting from a data breach. Public discussion of data breaches have focused on data exposure (the possibility that data has caused harm) as opposed to actual incidents of identity theft. The recently publicized figure that 100 million people have experienced data breaches does not mean that all 100 million people are victims of identity theft. As a case in point, ID Analytics has published research findings on an analysis of the entire breach file of four data breaches involving approximately 500,000 identities. It is noteworthy that only one data breach experienced misuse and the rate totaled less than .1% of the breach population. While ongoing monitoring remains necessary, the other three breaches were clear of fraudulent activity.

A one-size-fits-all approach to data breaches creates unnecessary public alarm as well as misallocation of fraud prevention resources. In reality, a lost or stolen laptop poses a far different risk of harm than a breach involving a targeted attack of a database of sensitive personal information. Harm assessments can focus attention on those breaches that truly pose a risk to the public and provide victim assistance directly to those needing it. Harm assessments can be used initially to determine if a breach has resulted in identity theft. On an ongoing basis, organizations can deploy breach analysis to monitor affected identities for possible misuse, so that any victims can receive expedited assistance, and thieves can be identified and stopped from further misusing the data.

### **PROTECT THE SOCIAL SECURITY NUMBER BY IMPROVING METHODS OF AUTHENTICATION:**

The Task Force has requested advice regarding the protection and treatment of Social Security numbers within government.



Rather than focus on Social Security numbers, we urge the Task Force to consider ways to improve authentication methods so they don't rely on personal information that is compromised or widely disseminated.

It would be a herculean task to remove the Social Security number from existing systems of government records and to otherwise cull the number from the public domain. Even if achievable, the benefits of such a costly effort should be questioned. Practically speaking, Social Security numbers have a diminishing value to fraudsters.

Most leading financial and wireless institutions now rely on anti-fraud tools, which will not validate an identity based on the mere presence of a Social Security number. Instead of looking at matches in data, these technologies look at how elements of identities behave and relate over time. The Social Security number is just one of many variables used to measure the validity of an identity.

While a legitimate Social Security number is needed to pass fraud checks of credit bureaus, fraudsters do not need to steal it to pass these checks. They merely, with a modicum of research, can cobble together a legitimate Social Security number. One easy method is called "Social Security number tumbling" where a fraudster modifies one digit of an existing number.

That's not to say Social Security numbers don't help combat identity theft. In some fraud prevention models, inclusion of Social Security numbers can increase the accuracy of the models by 19 percent. However, in other models, the credit applicant's home address and phone number – information that is publicly available - are more predictive of identifying theft than the Social Security number.

We fear efforts to restrict access to Social Security numbers will merely perpetuate the myth that the number still has value as a password. As an alternative, we would encourage regulators to restrict use of Social Security numbers as passwords for accounts. States like California and Colorado already prohibit companies from requiring a customer to use his or her Social Security number to access a website. Congress should generally prohibit the use of Social Security numbers as verifiers of identity. Moreover, Federal regulators should treat identity verification based solely on an SSN as an unsafe security practice.



These comments purely address efforts to restrict the use of Social Security numbers as part of an anti-fraud strategy. But there may be privacy reasons to restrict access to the number. Because the SSN is a unique identifier (not an authenticator), access to an individual's SSN could make it easier to create a dossier on that individual by facilitating the linking of databases.

**REGULATION SHOULD ALLOW THE PRIVATE SECTOR TO INNOVATE & COLLABORATE:**

We strongly encourage the Task Force to give organizations fighting identity theft the continued flexibility to adapt to the changing method of fraudsters. If we have learned one thing from fraudsters over the years, it is that they will constantly vary their techniques.

To that end, we are strong advocates for the value of data sharing among legitimate organizations in order to combat identity theft. Without data sharing, the best anti-fraud tools on the market today could not be built. ID Analytics and its consortium members stop literally thousands of identity thefts per month through the power of information sharing and collaboration.

Efforts to restrict data sharing will have the most effect on law abiding businesses. Criminals intent on identity theft will not hesitate to violate restrictions on data sharing, and will use any means available to get the tools they need to commit identity theft.

We thank the Task Force for this opportunity to present our views.

Sincerely,

A handwritten signature in black ink that reads "Thomas Oscherwitz".

Thomas Oscherwitz  
Vice President of Government Affairs  
ID Analytics