September 4, 2007

ID Analytics Response to the FTC Request for Comments on "Private Sector Use of SSNs"

Dear Commissioners:

ID Analytics appreciates this opportunity to comment on "Private Sector Use of the Social Security Number (SSN)."

ID Analytics is a leading provider of Identity Risk Management solutions and a pioneer in the field of risk-based identity scoring. Our technologies are used by many of the nation's largest wireless carriers and financial institutions, thousands of lenders, title and escrow companies, and by government agencies. Our comments will focus on the role of the SSN as an authenticator (topic 2), the role of SSNs in fraud prevention (topic 4), and the role of SSNs in identity theft (topic 5).

General Comments

We are submitting comments because we believe it is important to clarify the value and limitations of SSNs in assessing identity risk. SSNs are valuable inputs to fraud prevention systems – including ID Analytics' national ID Network® – but their value should not be overstated. The SSN is just one of many inputs to identity risk models. As a stand-alone authenticator, SSNs have extremely limited value because they are so widely available.

Efforts to regulate the SSN should also consider the costs of removing or restricting access to the number. SSNs, because of their historical use as unique record locators by commercial and government organizations, are embedded in countless record systems. We believe the cost of excising the number from these legacy databases and rebuilding the linkages provided by the number far outweighs the benefits in terms of identity protection.

As an alternative, we encourage Federal regulators to educate businesses about limitations of SSNs as authenticators. We also recommend that Federal regulators treat the practice of relying solely on the SSN to authenticate identity as an unsafe security practice.

The Use of the SSN as an Authenticator

We consider the SSN a poor stand-alone authenticator due to its wide public availability. SSNs and their associated names, addresses, and other personal information can be obtained in thousands of doctors' offices, financial institutions and other work sites around the country. Common facts about SSNs (including, for example, how to determine the state of issuance and approximate date of issuance) are made available by the Social Security Administration on its website. Entrepreneurs have taken this information and used it to create public web sites where any SSN may be entered and the user learns instantly if the SSN is valid, when it was issued, and where it was issued (see, for example, ssnvalidator.com).

The recent rash of publicly announced data breaches demonstrates how many SSNs are stored in business and government files. Since 2005, the Privacy Rights Clearinghouse has kept a running tab on identities compromised in data breaches. That number is now at 150 million, and many of these breaches were triggered by the compromise of SSNs.

The Role of The SSN in Fraud Prevention

In leading identity verification systems, SSNs function as inputs or linking keys used to predict identity verification of identity. In fraud prevention models built by ID Analytics, the inclusion of SSNs as model inputs have provided an increase in fraud detection performance of 10% to 20% over models built without use of SSN. But it must be stated that SSN is simply one of a diverse set of identity elements ID Analytics uses as part of its fraud prevention models. Other personal identity elements include name, address, date of birth, phone number, e-mail address, etc.; these are used along with transactional data elements such as date and time of transaction, source of transaction (internet, in-store, mall kiosk, etc.).

We have found that SSNs as a stand-alone variable are no more valuable than other identity elements, and in some cases are less predictive of identity risk. In internal ID Analytics' studies, the cross-industry linkages among identity risk events regarding a credit applicant's home address and phone number – publicly available data – have proven more predictive of identifying fraud than the SSN. Our identity risk scoring technology works extremely well at detecting fraudulent applications in the wireless industry even though 40% of applications for wireless service do not include (and in many cases do not even request) a SSN. We expect this SSN-less trend to continue to increase in the wireless and other non-financial industries. We also note that ID Analytics has built successful fraud prevention models in the United Kingdom where there is no commercially available equivalent to the SSN.

The Role of the SSN in Identity Theft

The principal reason why SSNs are useful in committing identity theft is that some companies and public sector entities still treat SSNs as proof of an individual's identity. Before gaining access to a commercial account – especially on the Internet – it is still too common for a consumer to be asked to supply a SSN as a user id or even worse as a password.

Concluding Recommendation:

Instead of restricting commercial use of SSNs, Federal regulators and Congress should put their effort into curbing their use as verifiers of identity (login, passwords, secret questions, etc.) which grant individuals access to services and other benefits. States like California and Colorado have the right idea. These states prohibit companies from requiring a customer to use his or her SSN to access a website. We would push this concept further. Congress should generally prohibit the use of SSNs as stand-alone authenticators of identity. Moreover, Federal regulators should treat authentication based solely on an SSN as an unsafe security practice.

We believe that SSN use by commercial companies will continue to diminish with the minor interventions stated above. This is a positive step. SSNs are issued by the government and are meant to last a lifetime. Once such an identity attribute is compromised, real difficulties face the holder of such a number because it is so hard to revoke, replace, or otherwise discard.

Thank you for your consideration.

Sincerely,
Thomas Oscherwitz
Vice President of Government Affairs and CPO
ID Analytics