



**Lisa A. Soda**  
Corporate Affairs Associate

**Corporate Affairs Department**

1220 L Street, NW  
Washington, DC 20005-4070  
USA  
Telephone 202-682-8590  
Fax 202-682-8207  
Email [sodal@api.org](mailto:sodal@api.org)  
www.api.org

September 5, 2007

Deborah Platt Majoras, Chairman  
Federal Trade Commission/Office of the Secretary  
Room H-135 (Annex K)  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

**SSNs In The Private Sector - Comment, Project No. P075414**

Dear Ms. Chairman:

The following represents comments from the Oil and Natural Gas Industry regarding use of Social Security Numbers (SSNs). The comments are being provided through the industry's trade organization, the American Petroleum Institute (API) in response to the Federal Trade Commission's (FTC) request to develop a "comprehensive record and the private sector's use of the SSN." API's Data Privacy Council coordinated this response.

The response begins with the questions the FTC posed in its request followed by an answer from the Oil and Natural Gas Industry.

**Topics for Comment:**

**1. *Current Private Sector Collection and Uses of the SSN***

- ✍ What businesses and organizations collect and use the SSN? For what specific purposes are they used?
- ✍ What is the life cycle (collection, use, transfer, storage and disposal) of the SSN within the businesses and organizations that use it?
- ✍ Are governmental mandates driving the private sector's use of the SSN?
- ✍ Are there alternatives to these uses of the SSN?
- ✍ What has been the impact of state laws restricting the use of the SSN on the private sector's use of the SSN?

SSN is used in the following instances in the oil and gas industry.

- ? Payroll/tax purposes
  - ✍ Employees
  - ✍ Retirees



- ✍ Shareholders
- ✍ Land owners (royalty payments)
- ✍ Contractors
- ✍ Beneficiaries
- ✍ Vendors
- ✍ Outsourced benefits systems
- ? Validating eligibility for employment
  - ✍ I-9 forms
  - ✍ Background checks
- ? Medical services and substance abuse testing
- ? Injury reports/Short term disability
- ? Passports and visas for flight crews.
- ? Internal identifiers
- ? Identity validation
  - ✍ Mostly being phased out (in favor of personnel or customer account number) but still used in certain business organizations (e.g. records management)
  - ✍ Likely to be present in historical records
- ? Credit card customers
- ? Third party litigants in the context of litigation management

SSN would be considered at the highest confidentiality level. Many companies will have standards in place that require encrypting SSN at least in transit (and potentially) at rest. SSN would be subject to the highest level of data destruction. SSN records are likely to be long life as the data will need to be maintained through the entire employment and retirement life cycle of individuals.

SSNs are used for a variety of purposes within the industry. The most obvious are for payroll and tax purposes. SSNs are collected from employees, retirees, shareholders, contractors and beneficiaries for payroll and tax purposes. These SSNs are also used within benefits systems which manage 401K and other funds. Some outside parties, namely land owners and some vendors, also provide SSNs to oil and gas companies for tax purposes. Land owners are individuals from whom oil and gas companies lease tracts of land for oil exploration/production. These individuals are given royalty payments for the exploration/production rights and consequently, their SSNs are required to meet tax obligations. SSNs are generally not accepted from vendors but small vendors may supply an SSN as their tax identification number on invoices and hence oil and gas companies working with these vendors would have these SSNs on file.

SSN is used during the employment application process to validate eligibility for employment and to facilitate background checks. The employment eligibility is handled through the I-9 form which is mailed to prospective employees prior to their employment. The new employee will bring the completed form on his/her first day along with supporting documentation (which may include a Social Security card, driver's license, passport, or other permissible documents) demonstrating his/her status. Once the documents are verified, the



completed I-9 may be included in the Personnel File (although best practice is to retain in a separate file) and maintained according to company retention guidelines.

SSN requested on employment application and Fair Credit Trading & Disclosure forms so that companies may conduct background check of prospective employees. SSN is used as a reference on reported back results.

Some medical providers require SSN for services provided. SSN is used as a reference from drug screen results reported back to the company from the third party vendor. SSN is also used on injury reporting and short term disability forms.

Internal corporate aviation departments collect SSNs of their crews to facilitate obtaining passports and visas. The SSNs are kept in a password-protected document and updated as personnel changes occur.

SSN was extensively used in the past to validate identity (ensure the appropriate person attended a required training class or was requesting a secure operation (password reset) from a help desk) and distinguish between employees who have similar names. For the most part, SSN has been phased out of these uses (in favor of an internally generated employee number or other internally set number) although there are still some pockets where SSN is used.

As SSN was historically used as an identifier and some of the documents on which SSN appears are company records, there is likely a significant presence of SSNs in company record stores and other documents which must be kept until their retention date expires.

SSNs are collected from credit card applicants for two reasons. One is to meet Patriot Act provisions regarding prevention of money laundering and international cash flow. There is a need to confirm the identity of the customer and SSN is apparently the easiest way to do this. The other reason is to check the applicant's credit history with a national credit bureau while processing the application.

Some litigation discovery processes require the use of SSN as an authenticator in order to obtain relevant discovery records of the claimant (i.e. subpoena for medical or tax records). In addition, SSN helps identify claimants who file the same claim in multiple jurisdictions.

Government mandates certainly drive some of the use of SSNs within the oil and gas industry. The most obvious is the collection of the SSN for tax purposes. The Patriot Act looks to be at least a partial contributor to the collection of SSN from credit card applicants. SSNs are required to acquire passports and/or visas. Some states also require SSNs in some circumstances, the State of California (California Code of Regulations, Title 8 Section 14004 Form 5020) requires the SSN on workplace injury reports that are reported to the state.

In many cases, the SSN is not necessarily required although it may be the easiest means of meeting the objective. The Patriot Act, for example, allows use of other identifiers (like a

Tax Identification Number (TIN)) instead of an SSN but many individuals (with whom one is dealing with credit card applications) effectively use their SSN as their TIN. Many benefits systems use the SSN as a login identifier; while it would seem that something else could easily be substituted as a login identifier, these systems still need the SSN for tax purposes and would have to have the number on file anyway. In places where other identifiers are available (internal authentication), many companies in the industry have begun to move away from using SSNs.

There hasn't been much impact from state legislation restricting use of SSN. As noted above, some states require SSN on some forms that are sent to the states. There was a flurry of effort to craft appropriate privacy policies when Texas HB 1130 was passed a couple of years ago.

## 2. *The Role of the SSN as an Authenticator*

- ✍ The use of the SSN as an authenticator – as proof that consumers are who they say they are – is widely viewed as exacerbating the risk of identity theft. What are the circumstances in which the SSN is used as an authenticator?
- ✍ Are SSNs so widely available that they should never be used as an authenticator?
- ✍ What are the costs or other challenges associated with eliminating the use of the SSN as an authenticator?

SSN is rarely used as an authenticator. Exceptions include: within the credit card application as required by the Patriot Act, and as an optional voluntary identifier for call-in authentications (in conjunction with other forms of identification).

Some litigation discovery processes require the use of SSN as an authenticator in order to obtain relevant discovery records of the claimant (i.e.- subpoena for medical or tax records). In addition, SSN helps identify claimants who file the same claim in multiple jurisdictions.

Eliminating SSN as an authenticator could be present challenges in obtaining documents during litigation or in identifying a litigant who has filed the same claim in more than one jurisdiction. Litigants can have identical names and sometimes birthdates, and facilities need to be able to distinguish between individuals when creating, maintaining and/or locating records

## 3. *The SSN as an Internal Identifier*

- ✍ Some members of the private sector use the SSN as an internal identifier (e.g. employee or customer number), but others no longer use the SSN for that purpose. What have been the costs for private sector entities that have moved away from using the SSN as an internal identifier? What challenges have these entities faced in substituting another identifier for the SSN? How long have such transitions taken? Do those entities still use the SSN to communicate with other private sector entities and government about their customers or members?

- ✍ For entities that have not moved away from using the SSN as an internal identifier, what are the barriers to doing so?

The costs from switching from SSN as an internal identifier can vary. In cases where SSN was used as an internal identifier (proof of mandatory class attendance, as an example), the change could be effected by simply changing the form, process, and/or documentation. The case of switching off SSN as an employee/customer number, though, is far more complicated. From a technical aspect, the database storing the information would likely need to be redesigned and built as SSN would likely to have been the primary (if not only) key for accessing records. This change would likely precipitate other changes in application “downstream” from the initial database which might use or feed the data. New processes also would likely to be needed particularly in handling possible duplication of records. As SSN is unique to a particular individual, it can be used to distinguish between employees with similar (identical) names. An employee number, assigned as a person is entered in the database, cannot do this and consequently other (personal) information (birth date, birth place, citizenship, etc.) will be needed to avoid duplicating records.

Depending upon how well SSN is integrated into the process, the change could be quite costly and time consuming.

The industry does not have any recent experience in converting a human resources system off of SSN as a key and cannot provide any relevant cost numbers along those lines.

#### 4. *The Role of the SSN in Fraud Prevention*

- ✍ Many segments of the private sector use the SSN for fraud prevention, or, in other words, to prevent identity theft. How is the SSN used in fraud prevention?
- ✍ Are alternatives to the SSN available for this purpose? Are those alternatives as effective as using the SSN?
- ✍ If the use of the SSN by other sectors of the economy were limited or restricted, what would the ramifications be for fraud prevention?

Alone, an SSN cannot be used for ID theft/ fraud prevention. Multi-factor authentication remains a more secure means of identifying individuals. Although alternative methods are being examined, currently, SSN, coupled with additional authentication information, remains the truest means of identification. As the use of SSN becomes more restricted, it is certain the preferred replacement piece of ID will become the next target for ID thieves. Thus, fraud may appear to decrease for a time, but is expected to rise again as the SSN is replaced with other ID forms/ alternatives.

#### 5. *The Role of the SSN in Identity Theft*

- ✍ How do identity thieves obtain SSNs?
- ✍ Which private sector uses of the SSN do thieves exploit to obtain SSNs, i.e., SSN as identifier or SSN as an authenticator? Which of those uses are most vulnerable to identity thieves?



- ✍ Once thieves obtain SSNs, how do they use them to commit identity theft? What types of identity theft are thieves able to commit with the SSN? Do thieves need other information in conjunction with the SSN to commit identity theft? If so, what other kinds of information must they have?
- ✍ Where alternatives to the SSN are available, what kind of identity theft risks do they present, if any?

Based on news reports, it would seem that thieves can obtain SSNs through a variety of methods including social engineering, laptop theft, and insider access. The latter two can be mitigated to some extent by appropriate security protections (like encryption).

Using SSN as an identifier probably provided the most exposure as a thief could have just looked at a class sign-up sheet, performance evaluation, or any of a number of forms where the number was present. As noted above, most companies have phased out use of the SSN from these uses.

The oil and natural gas industry is not qualified to answer the question as to how thieves use the SSN to commit identity theft.

Regarding alternatives, a danger is that one would simply replace the SSN with another number which is used similarly. This would simply transfer the problem from the SSN to the new number.

Sincerely,

Lisa A. Soda  
Corporate Affairs Associate