August 21, 2007

Federal Trade Commission
Office of the Secretary, Room H-13 (Annex K)
600 Pennsylvania Avenue N.W.
Washington, DC 20580

Subject: Social Security Numbers (SSNs) in the Private Sector – Comment, Project No. P075414

Dear Sir or Madam:

Boeing Employees' Credit Union (BECU) appreciates the opportunity to offer input and comments on the topic of SSNs in the Private Sector. BECU is a state-chartered, federally insured credit union with assets of $7.5 billion and a membership base of over 500,000.

Let us begin by saying we applaud your continuous efforts to address and combat identity theft and the resources you provide the public on this growing issue. Everyday BECU encounters a consumer who has been a victim of identity theft and the steps the consumer has to endure to try to clear up their records. We recommend your website to our members for the valuable information and resources you have available.

Here is our input and comments on the specific questions you asked.

Current Private Sector Collection and Uses of the SSN

1. What businesses and organizations collect and use the SSN?
Just to name a few: credit unions, financial institutions in general, consumer credit reporting agencies, and employers of all US companies.

2. For what specific purposes are they used?
We, as a financial institution, use SSNs in the following ways:

- *To comply with our Bank Secrecy Act Customer Identification Program,*
- *To determine membership with our credit union eligibility based on credit and debit history,*
- *To establish loans (by providing the SSN to the credit reporting agency(s)),*
- *For identification when determining a possible false-positive related to an Office of Foreign Assets Control hit,*
- *Investigations surrounding fraud and identity theft,*
- *For debt collection purposes,*
- *To verify the member when conducting financial transactions,*
- *Reporting of interest information to the IRS.*

As an employer:

- *For payroll purposes and reporting of income and taxes to the IRS.*

3. What is the life cycle (collection, use, transfer, storage and disposal) of the SSN within the businesses and organizations that use it?
It is collected for opening accounts as indicated in question two. It is stored in databases, image files, and on printed paper. Where and when technically possible in the database or image file systems it is encrypted. It is further used when new products are requested that require credit checks and consequently is transferred to one of the three consumer credit reporting agencies. Transfer to other third party partn

more than just money
BECU

is restricted and when required, it is closely monitored. In many cases disposal is restricted by governing body regulations, for example, membership applications.

4. Are governmental mandates driving the private sector's use of the SSN?
Partially. The Bank Secrecy Act (BSA) has rules that rely heavily in the use and verification of it. Fraud and new account processes, which are not necessarily mandated by the regulators, do not need the SSN as many of our new account opening products rely on it to establish membership, which is mandated by the BSA.

5. Are there alternatives to these uses of the SSN?
Not always. When it comes to identifying members of society across organizational lines there is no single unified identifier. For example, a unique identifier assigned to a customer of one organization would not match that of another organization's unique identifier. Checking credit is the biggest hurdle to reducing the use of SSN in the private sector. If efforts were aimed at using an alternate identifier, it too will become the target of identity thieves. We don't have any issues with the requirement of the SSN. We feel it is an important identifier that financial institutions need to validate identity.

6. What has been the impact of state laws restricting the use of the SSN on the private sector's use of the SSN?
It has caused many organizations to stop using SSNs as the primary identifier for access to Internet-facing applications, which is a positive effect. Reducing the use of the SSN for Internet-facing applications should be continued.

<u>The Role of the SSN as an Authenticator</u>
7.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?
We use the SSN in the following instances:

- *In the new account opening process including our Customer Identification Process as required in the BSA rules.*
- *In investigations related to claims of identity theft and financial fraud,*
- *Hits to the Office of Foreign Assets Control list,*
- *Credit checks on loan applications,*
- *Member verifications.*

8. Are SSNs so widely available that they should never be used as an authenticator?
It should not be allowed as an Internet-facing application identity credential. We feel no private sector organization should be allowed to use it as an element for Internet application authentication. However, we do feel the requirement of the SSN is necessary in other factors; such as verification. We don't feel it should solely be relied upon for verification, but that in conjunction with other validating information, it is effective.

9. What are the costs or other challenges associated with eliminating the use of the SSN as an authenticator?
This is not a single business entity issue and cannot be done without cross entity cooperation. How would private sector business entities identify the same individuals – credit checking again would be the biggest challenge for us. Again, regulating the use of the SSN as an authenticator for Internet-facing applications should continue. Our ability to compare credit and debit history to determine a possible fraudulent new member would not be effective and would increase our fraud losses. Without knowing what other identifiers

the government is reviewing, it is hard to determine how we would fulfill our obligation of knowing our member.

10. Some members of the private sector use the SSN as an internal identifier (for example, an 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?

We have transitioned our computer systems from using the SSN as the member identifier, to a unique, system-generated member number. Removing the SSN as the identifier and just relying on it for authentication was a necessary and prudent step for our members and our business. When collaborating with other private sector entities or government agencies, after taking appropriate precautions of course, we utilize SSN as an identifier, because our internal identification number would not align or could not support cross referencing, with other private sector entities or government agencies unique identifiers.

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

Costs. In many cases, moving away from SSNs would require adopting entirely new systems. Additionally, there is staff and member training/education. When we switched our computer systems over to not use the SSN as the account number, some of our members had a difficult time adjusting – as with any change. Additionally, we had at least a year's worth of newsletter articles provided to our members and advanced training to staff. It had been delayed once as we wanted to ensure a smooth transition to our members.

The Role of the SSN in Fraud Prevention

12. 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?

Primarily it is used as a second factor of authentication – something that one knows about him/herself that others should not know. Today of course we only ask for the last four digits. When we open new accounts we use it by entering the number when we pull credit and debit history.

13. Are alternatives to the SSN available for this purpose? Are those alternatives as effective as using the SSN?

We believe so. We use code words and other data elements as second factor forms of authentication, however, because we are not in physical proximity we can't always check photo identification subsequently we rely on our members to provide us three elements that only they should know about themselves (e.g. date of birth, last four digits of the SSN, code word, etc.). However, when we pull credit history for new accounts and loans, there isn't another identifier we would feel comfortable using for verification.

14. If the use of the SSN by other sectors of the economy were limited or restricted, what would the ramifications be for fraud prevention?

Regulating the use of the SSN by the private sector is a prudent control measure and should be pursued further. With that said, any new identifier used for financial credit history will be targeted by identity thieves. Consequently, and more importantly, regulations requiring the protection of SSN or any other unique identifier should be the focus of the FTC and other regulatory agencies. However, if the use is restricted to other sectors, and not us, we would still use it. This would promote conversations with our members, potentially unpleasant, as they would question why we would still require the use of it but other sectors don't.

The Role of the SSN in Identity Theft

15. How do identity thieves obtain SSNs?
The ways for gaining a SSN are numerous. Here are a few: Internet search engines, theft of mail, dumpster diving, database breaches, computer theft, key-stroke loggers, spy ware, social engineering such as phishing, vishing, 419 scams and even internal plants at companies. Additionally, we have found where family members have stolen a relative's SSN and open accounts, credit, etc.

16. Which private sector uses of the SSN do thieves exploit to obtain SSNs, (for example, the SSN as an identifier or SSN as an authenticator)? Which of those uses are most vulnerable to identity thieves?
These two uses are equal at risk. A thief may, for example, overhear a phone conversation where a consumer is asked for their SSN whether the use is as an identifier or authentication factor. When the SSN is used as an authenticator, we feel limiting and regulating private sector entities to use only the last four would be a prudent control.

17. 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?
Typically, other data elements are needed by identity thieves to truly assume a consumer's identity. If a thief gains a consumer's SSN they will use it in attempt to gain the other data elements to complete the identity theft. A thief may call a private sector entity armed with the SSN and attempt to social engineer the other elements such as date of birth, address, mother's maiden name, driver's license number, etc. Most of this information can be obtained through various internet searches, phishing, vishing, etc. After gathering this information, they establish or takeover bank accounts, credit cards, auto loans, home loans, lines of credit, etc.

18. Where alternatives to the SSN are available, what kind of identity theft risks do they present, if any?
We believe that whatever changes are made, there may be impact and reduction initially, but as the thieves regroup, we will be back to where we are in regards to fraud and loss. Any new identifier used for financial credit history will be targeted by identity thieves. Consequently, and more importantly, regulations requiring the protection of the SSN or any other unique identifier should be the focus of the FTC and other regulatory agencies.

Thank you for allowing us the opportunity to provide comments.

Sincerely,

President and CEO