



JAMES P. GHIGLIERI, JR.
Chairman

CYNTHIA BLANKENSHIP
Chairman-Elect

R. MICHAEL MENZIES
Vice Chairman

KEN F. PARSONS, SR.
Treasurer

WILLIAM C. ROSACKER
Secretary

TERRY J. JORDE
Immediate Past Chairman

CAMDEN R. FINE
President and CEO

September 5, 2007

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

Re: SSNs in The Private Sector – Comment, Project No. P075414

Dear Sir or Madam:

The Independent Community Bankers of America (ICBA)¹ appreciates the opportunity to comment on private sector uses of Social Security Numbers (SSNs) for the study being conducted for the President's Identity Theft Task Force.

ICBA applauds these efforts. Identity theft is a growing problem in the United States. Community banks take their responsibilities very seriously and take steps to ensure the security of customer information and protect customers from identity theft. While community banks rely on the use of Social Security Numbers for many reasons, ICBA also believes that appropriate restrictions may be useful to help stem the tide of identity theft. However, any restrictions must be carefully evaluated. Overly broad restrictions will have unintended consequences and possibly help fraudsters and identity thieves by creating barriers to proper identification and authentication of community bank customers.

¹ The Independent Community Bankers of America represents 5,000 community banks of all sizes and charter types throughout the United States and is dedicated exclusively to representing the interests of the community banking industry and the communities and customers we serve. ICBA aggregates the power of its members to provide a voice for community banking interests in Washington, resources to enhance community bank education and marketability, and profitability options to help community banks compete in an ever-changing marketplace.

With nearly 5,000 members, representing more than 18,000 locations nationwide and employing over 268,000 Americans, ICBA members hold more than \$908 billion in assets, \$726 billion in deposits, and more than \$619 billion in loans to consumers, small businesses and the agricultural community. For more information, visit ICBA's website at www.icba.org.

Current Private Sector Collection and Uses of the SSN

1. What businesses and organizations collect and use the SSN?

Along with other financial institutions, community banks collect and use customers' Social Security Numbers for a variety of reasons.

2. For what specific purposes are they used?

For many years, community banks and other financial institutions have collected SSNs to comply with federal and state statutes. For example, the SSN is used for appropriate Internal Revenue Service reporting. The SSN is also used to comply with the requirements of the USA PATRIOT Act. Section 326 of the Patriot Act, as implemented by the U. S. Treasury Department and the federal banking agencies, requires community banks and other financial institutions to establish customer identification programs. One of the statutory provisions Congress established requires banks to obtain a customer's SSN. In addition, the SSN is used as an identifier on other Treasury forms, including Suspicious Activity Reports and Currency Transaction Reports as well as state Uniform Commercial Code filings.

SSNs are also used as an identifier for credit bureau information reporting and retrieval purposes. Because a SSN is unique, it can help ensure that information about a specific individual is properly connected to the correct credit data. For example, there may be two individuals with similar or identical names residing at the same address, such as a father and son. The SSN helps distinguish the two.

Community banks and other financial institutions frequently use the SSN as a unique internal identifier for the same reasons mentioned in the previous paragraph.

3. What is the life cycle (collection, use, transfer, storage and disposal) of the SSN within the businesses and organizations that use it?

As with many other bank records, the information on customers – including their SSN – is maintained as long as an account is open and then for 5 to 7 years after the account is closed. However, under requirements established by the Gramm Leach Bliley Act and the Fair and Accurate Credit Transactions Act of 2003, along with the implementing rules issued by the federal banking agencies, community banks must ensure that these records are transferred, stored and disposed of only in appropriate ways to ensure the information does not inadvertently become available to fraudsters and identity thieves.²

² For example, under the *Guidelines Establishing Standards for Safeguarding Customer Information* issued by the federal bank regulators in March 2001, community banks must establish appropriate administrative, technical and physical safeguards for customer records and information in order to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. In carrying out these requirements, community banks must identify and assess risks that may threaten customer information, develop a written plan containing policies and procedures to manage and control these risks, implement

4. *Are governmental mandates driving the private sector's use of the SSN?*

As noted above, various statutory requirements – both state and federal – require community banks to collect and maintain SSNs.

5. *Are there alternatives to these uses of the SSN?*

In many instances noted above, use of the SSN is mandated by statute.

While some have suggested that use of the SSN could be eliminated from credit report data, doing so would be an expensive and burdensome proposition that is unlikely to accomplish the goal of reducing identity theft. If the SSN were eliminated from credit bureau data, the credit bureaus would have to develop an alternative system to identify individuals. Developing this alternative would be costly and time consuming. In the interim, the difficulties associated with identifying individuals might actually facilitate identity theft. And, once an alternative identifier is established for credit reporting, that alternative would be just as susceptible to abuse by identity thieves as the existing use of SSNs for credit reporting.

6. *What has been the impact of state laws restricting the use of the SSN on the private sector's use of the SSN?*

For the most part, state restrictions do not seem to have had an extensive impact on community banks. While some community banks may have used SSNs at one time in deposit account numbers, just as some states used the SSN for a driver's license number, that practice appears to have been eliminated for the most part.

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.

7. *What are the circumstances in which the SSN is used as an authenticator?*

Community banks and other financial institutions may rely on a customer's SSN or the last four digits of the SSN to authenticate that customer's identity. For example, the SSN or the last four digits can be used to verify identity when customers are using telephone or online banking applications, including call centers, to make account inquiries, access account information or conduct account transactions.

8. *Are SSNs so widely available that they should never be used as an authenticator?*

Community banks and other financial institutions should continue to have the flexibility to use a customer's SSN or the last four digits as a simple means of authenticating a customer's identity as long as appropriate safeguards are taken, as required under existing laws and implementing rules.

and test the plan, and adjust the plan on a continuing basis to account for changes in technology, sensitivity of customer information and internal or external threats to information security.

9. *What are the costs or other challenges associated with eliminating the use of the SSN as an authenticator?*

As noted above, replacing the Social Security Number as an identifier or authenticator would be a costly undertaking. Moreover, since a complete new system for identification would have to be developed, especially for credit reporting purposes, the alternative would eventually become as susceptible to identity theft as the SSN. Community banks already take steps to ensure the information is properly protected, as required by federal law and regulation.

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.

10. *What have been the costs to move away from using the SSN as an internal identifier?*

Moving away from using SSNs as account numbers does not appear to have been a problem for most community banks.

11. *What challenges apply when substituting another identifier for the SSN?*

Substituting an alternative identifier would require careful attention to detail in the transition to ensure that all records are changed in an accurate and timely way. This would be both expensive and time consuming.

12. *How long have such transitions taken?*

That data is not available.

13. *Do those entities still use the SSN to communicate with other private sector entities and government about their customers or members?*

As noted above, the SSN is used to file various reports with federal and state governments, including tax reporting, UCC filings, and various Treasury reports such as Suspicious Activity Reports and Currency Transaction Reports. The SSN is also used for Patriot Act section 314(a) data-matching, a system used by federal law enforcement agencies acting through Treasury's Financial Crimes Enforcement Network (FinCEN) to track information on possible money launderers or terrorist financiers. And, the SSN is used for credit bureau reporting.

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.

14. *How is the SSN used in fraud prevention?*

Currently, the SSN is used as a verifier through software packages. These programs, such as "Searchbug," will confirm if the SSN belongs to a deceased person, if it is active, in what state the number was originally issued and confirm date of birth. It is our understanding that the Social Security Administration is working on developing a

similar program that could be used by financial institutions to verify identity and the validity of an SSN.

15. Are alternatives to the SSN available for this purpose?

Since many of the current fraud detection systems are based on the SSN, it is not known if alternatives are currently available. However, as with credit reporting, developing an alternative would be a costly and burdensome proposition.

16. Are those alternatives as effective as using the SSN?

To be as effective as the SSN, any alternative unique identifier would have to be as widely used and accepted. And, creating an alternative identifier would merely replace the SSN with a new number that would be used in virtually the same way as the SSN is used today.

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

Creating an alternative would make it more difficult for identity thieves. However, it would also make it more difficult for community banks to identify customers. This would become a barrier to fraud prevention.

The Role of the SSN in Identity Theft

18. How do identity thieves obtain SSNs?

There are many ways that identity thieves can obtain SSNs. For example, one common method is “dumpster diving” for improperly disposed records. However, community banks are required by federal law and regulation to ensure that records are disposed properly.

In many instances, SSN information is publicly available. For example, many local communities post tax and real estate records online where the information posted includes an individual’s SSN. In addition, oil and gas lease records that are readily available to the public may include SSNs.

Another mechanism for identity thieves to obtain SSNs is through computer hacking and data breaches. However, community banks are required by federal law and regulation to take appropriate steps to ensure data security.

19. Which private sector uses of the SSN do thieves exploit to obtain SSNs, i.e., SSN as identifier or SSN as an authenticator?

Among other means, identity thieves might exploit SSNs printed on checks (a practice community banks discourage), improperly disposed records that include SSNs, or old identification cards such as driver’s license or medical insurance cards that use SSNs that consumer fail to properly dispose.

20. Which of those uses are most vulnerable to identity thieves?

The printing of SSNs on checks (a practice community banks discourage) is probably the practice most vulnerable to identity thieves.

21. Once thieves obtain SSNs, how do they use them to commit identity theft?

There are a number of means that identity thieves use to exploit the SSN. For community bank accounts, the numbers can be abused to apply for credit cards or other accounts or obtain a replacement card on an existing account.

22. What types of identity theft are thieves able to commit with the SSN?

The SSN can be exploited to charge merchandise or make other purchases on a credit card, using the SSN as an identifier on an existing account. Similarly, the SSN can be used to obtain cash advances against an existing credit card. Access to the SSN, along with other identifying information, can help “validate” the identity of the individual. However, it is important to recognize that current laws and card company procedures greatly restrict the liability of a cardholder in situations like this. For example, many card companies provide zero liability for the cardholder, and card company rules require extra steps to be taken where the actual card is not present for a transaction.

23. Do thieves need other information in conjunction with the SSN to commit identity theft?

An identity thief would need other identifying information, such as name and address, along with the SSN. Federal banking regulators, though, regularly issue guidance for community banks to ensure that appropriate steps are taken to ensure that an individual is in fact who he or she claims to be, including the use of biometrics and other data. Where the risk increases, community banks are expected to and do take additional steps to authenticate an individual’s identity. Moreover, to protect against both financial loss and damage to the bank’s reputation, banks have a vested interest in implementing and ensuring these measures are effective.

24. If so, what other kinds of information must they have?

In addition to a SSN, community banks may require information such as the date of birth, last known address or other identifiers. Federal Financial Institutions Examination Council (FFIEC) guidelines issued in October 2005³ outline three types of information that can be used to more accurately authenticate someone’s identity: something the person knows (such as a personal identification number or password), something the person has (such as a credit card or ATM card), and something the person is (a biometric such as a fingerprint).

25. Where alternatives to the SSN are available, what kind of identity theft risks do they present, if any?

As noted above, any alternative that is developed to replace a SSN will eventually be subject to the same problems that are faced with the use of the SSN. And, developing an alternative will be costly, confusing and, during the transition period, will actually make it easier for identity thieves to exploit vulnerabilities in the system.

³ See, e.g., FDIC FIL-103-2005.

Thank you for the opportunity to comment. If you have any questions or would like additional information, please feel free to contact the undersigned at 202-659-8111 or by e-mail at robert.rowe@icba.org.

ICBA looks forward to continuing to work with the Federal Trade Commission and other agencies to combat identity theft and to identify reasonable and effective ways to address the problem.

Sincerely,

A handwritten signature in black ink that reads "Robert G. Rowe" with a stylized flourish at the end.

Robert G. Rowe, III
Regulatory Counsel