Statement of Rob Evans

Director of Industry Marketing, NCR Corporation

Testimony Before the

Senate Subcommittee on Social Security and Family Policy

On

Thursday, July 11, 2002

In

Dirksen Senate Office Building, Room 219

At

2:00 P.M.

S. 848, "The Social Security Number Misuse Prevention Act of 2001" – Protecting the Social Security Number: an issue of privacy or security?

Chairman Breaux, Senator Grassley, and members of the Subcommittee, my name is Rob Evans, Director of Financial Industry Marketing for the NCR Corporation. Thank you for the invitation to offer testimony today before your Subcommittee.

The company I represent, the NCR Corporation based in Dayton, Ohio, is the worlds leading manufacturer of ATMs. We also design, manufacture, and integrate a variety of specific purpose financial terminals for our banking customers. In my current capacity, I have the opportunity to interface with our Americas based customers who need to process self-service financial transactions in an efficient, secure, and reliable environment. In addition to our financial business unit, NCR has a proud heritage in retail transaction processing and also includes our Teradata Solutions Group which provides database management solutions and general purpose computing products to global customers.

NCR's history in providing solutions for the financial industry extends back to the initial development of magnetic ink character recognition (MICR) based solutions for check clearing and the use of single number account control, or SNAC based transaction processing. Not only are our earliest products featured in Smithsonian collections (the museum of American history Numismatic collection), but our modern solutions are being deployed by cutting edge institutions in every corner of the globe as we speak. The NCR Corporation currently employs over 31,000 people globally.

Mr. Chairman, while the subject of today's hearing is "Protecting the Social Security Number", the fundamental issue is protecting our shared confidence. Confidence in

payment mechanisms, confidence in ubiquity and acceptance, and confidence in individual security and privacy. Without the confidence that significant financial transactions can be negotiated with both efficiency and security, we will continue to witness gradual erosion in consumer confidence. And as significant from a business point of view, we will fail to realize the significant economic benefits that improving technology and quick response to consumer financial needs can bring.

However, balance demands that we do our utmost to protect vital information belonging to individual customers. A diminished ability for consumers to obtain credit due to identity theft or fraud will be as chilling to economic activity as a diminished ability to grant credit due to cumbersome processing. While I do not particularly envy the task of the subcommittee, you are to be thanked for taking the initiative to strike a balance while improving the security of social security numbers.

According to independent industry analysts, 200 million applications for credit were processed as recently as 1997. Outstanding balances from the top ten United States issuers of "general purpose" credit cards reached $387 billion in 1999, and represented 11% growth in one years' time. While mortgage refinancing represents a significant portion of the nations mortgage business, second mortgages, home equity lines of credit or HELOCs, and debt consolidation offers continue to grow in volume. These consumer credit obligations, as well as revolving credit, can be issued using not much more than the postal service and a social security number. Clearly, the need to improve the security of consumers social security numbers is increasing with these industry figures.

Numerous organizations have recognized the need to enhance and increase the security levels associated with identification methods and credit instruments. Recently, the Department of Defense begun to reissue identification cards leveraging chip based smart card technologies. In Europe, VISA are pursuing EMV based card and card reading solutions to make fraudulent duplication more difficult. In Asia, MasterCard is testing a user fingerprint embedded in magnetic slurry to ensure authorized use. While all these systems do a better job tying individuals to account numbers and authorization IDs, they are predicated on specific chip or stripe reading technologies which are not presently ubiquitous. And while the advent of technology which may find chip readers in every telephone is promising, it is far from immediate. Unfortunately, the need secure social security numbers is present.

The fundamental problem the committee will encounter is not entirely dis-similar to that which ATM owners and operators face. Specifically, how can we be certain that the individual presenting them self to transact business on a particular account is indeed authorized to do so? While not foolproof, the methods currently employed by ATMs may bear review for potential use with social security numbers. The card and PIN system functions well in its limited capacity. Specifically, a social security number could function as the card, and a PIN assignment to the number would add a level of security.

A system could be built and managed which generates authorizations for applications of credit above a specified significant dollar value. The authorizations would be issued and

verifications returned by a system which allows credit issuers to pass through authenticated requests. A conceptual diagram is attached for your review.

Is such a system, as described, absolutely foolproof? No, it is not. It does, however, offer a more secure environment for the use of social security numbers in significant financial transactions. It is analogous to car locks on your car door. The lock is not a guarantee that the car will never be stolen, but the average consumer would not dream of purchasing a car that didn't have locks. This system could be activated and utilized via touch tone telephone, giving it a degree of ubiquity necessary for minimum disruption in current processes. While this system will not guarantee unauthorized use, it would make unauthorized use more difficult.

Current transaction processing and switching technologies could handle the volume of requests in the system today. The nations ATM infrastructure switches nearly 12 billion transactions annually, as a point of reference. The cost would depend on how the process is defined. For example, advance notifications of revised procedures and processes should be required, and a re-issue of social security number cards would be desired with PINs sent in separate mailings. These start up costs in addition to the switching technology could average in the teens of dollars per account. The ongoing operating costs could be dollars per account on a speculative basis.

There are problems with the conceptual model defined. Ensuring data integrity over the phone system via encryption of sensitive data would be desirable but is not present in the

conceptual model. In current ATM systems, the bank who holds the account processes the PIN. This process is defined as a third party PIN issuer in the conceptual model, but the designated trusted third party would doubtlessly need to develop methods to ensure confidentiality and security of PINs and account numbers.

NCR applauds the committee for its work on this sensitive subject. NCR appreciates the need for solutions which support the integrity of the current social security numbering infrastructure but add security mechanisms for individual account holders. NCR is ready to assist the committee in working on specific technical issues surrounding security in addition to assistance in developing and defining solutions as well.

Mr. Chairman, thank you and the committee very much for your time and attention to this matter.