Background

In 2002, identity theft topped the Federal Trade Commission's list of received complaints for the third consecutive year, with the total number of incidents doubling from the previous year. In a typical case of identity theft, a criminal uses his or her victim's Social Security Number (SSN) to obtain credit cards or loans in the victim's name. This not only costs the credit card and loan issuers money when the criminal defaults, but can also severely harm the credit rating of the victim whom often must spend hundreds of hours trying to remove the false information from their credit report. According to studies by the U.S. General Accounting Office, this class of fraud costs hundreds of millions of dollars each year. A similar potential identity theft problem occurs when a criminal gives the victim's personal information to law enforcement after being arrested. The crimes (and any missed court dates) go on the victim's criminal record and can lead to arrests based on this misinformation. The best way to prevent identity theft is to protect personal information, in particular the Social Security Number.

Most employees are required to pay a certain percentage of their earnings to the Social Security system through the Federal Insurance Compensation Act (the FICA tax). The Social Security Number was created to ensure that an individual's earnings and FICA taxes are properly recorded. Since the Social Security Number is the primary means of identifying an individual for purposes of tax or earnings reporting, it will continue to be required information for Duke employment, student financial aid, transactions which require reporting to federal agencies, and as a business necessity for certain departments.

Considering the intended purpose of the SSN and the potential for identity theft if it is not properly maintained, several state legislatures have passed laws limiting the use of student Social Security Numbers at all levels of public and private educational institutions. Furthermore, most states have stopped using Social Security numbers in such documents as driver's licenses. Advocating for protections against identity theft nationwide, Senators Dianne Feinstein and Judd Gregg have introduced the Social Security Number Misuse Prevention Act [1], which, if passed into law, would restrict public access to SSNs -- removing them from government checks, marriage licenses, public records and many other legal documents where they are currently used for identification.

Social Security Number use at Duke University

Like many other institutions, both corporate and educational, Duke uses the Social Security Number for many purposes for which it was not originally intended, such as to uniquely verify a person's identity. This use creates at least two problems for Duke:

- SSNs are not actually very good identifiers. For example, not all members of the Duke community have SSNs when they arrive at Duke. In trying to accommodate this problem, Duke often creates artificial SSNs, which may later be replaced when the government issues a SSN for tax purposes. This, coupled with the fact that Social Security Numbers can be changed (for example in the event of identity theft or domestic violence) creates the potential for confusion in any system that relies on them for identifying individuals.

- Having SSNs in our computer systems creates additional vulnerability. Over the past few years there have been several incidents of computerized theft of SSNs from different universities. The number of universities involved indicates that criminals are actively trying to exploit such systems in order to gain personal information about faculty, staff and students. The largest (and most recent) theft was that of over 55,000 Social Security Numbers (along with other personal information) from the University of Texas [2] [3].

A similar, but smaller, incident at Indiana University cost that institution both in terms of money and reputation [4]. The University was criticized in the local press for several months and ended up offering reimbursement for up to three credit reports for each individual affected [5]. The recent incident at the University of Texas looks as if it may result in similar costs.

In order to avoid mishaps with Social Security Numbers, similar to those of other institutions, it is important that we limit the use of the SSN wherever possible. This limited use of the Social Security Number can be accomplished by migrating to less sensitive forms of identification (and verification of identity) such as the Duke Unique ID and the Duke NetID. For
applications which still require social security numbers, we should make every attempt to ensure that this sensitive information is protected. This can be assured through the regular auditing of such systems.

**Proposed Action**

For the past several months, the Office of the CIO has been working to determine how extensively the Social Security Number is used at Duke with the goal of eliminating unnecessary uses. We have found many cases where SSNs are used by systems that do not have a strict need to maintain the SSN. We believe that by enacting a policy to protect SSNs, Duke can minimize the risk of being the source of information for identity theft (Duke would not be the first university to enact such a policy [6] [7]). Furthermore, by gradually phasing in this program we will be able to minimize the disruption to existing operations.

- Migrate, or implement plans to migrate, all services using the SSN as an identifier to the Duke Unique ID
- Identify systems or processes which use the SSN to verify a person's identity and migrate such systems to a stronger form of authentication
- Require departments using the SSN to:
  - show institutional need
  - receive approval from the Offices of the Executive Vice President and the Chief Information Officer
  - receive yearly audits of the system by the IT Security Office (including the server and application security) to ensure safe SSN handling
- Departments at Duke should cease the collection of Social Security numbers, except where there are legitimate requirements (e.g. financial aid, tax reporting, etc.)
- Duke’s Internal Audit Office should include in routine audits, the validation of departmental compliance with any established SSN policies and procedures.

By using alternatives to Social Security Numbers for identification and authentication, Duke will be able to safeguard personal data more effectively and will reduce the risk of identity theft for its students, faculty, staff and patients. Furthermore, using alternatives to the SSN will allow Duke to manage databases that refer to people in a more robust manner.

**References**

[1] [http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.00228](http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.00228)
[2] [http://www.utexas.edu/data/theft](http://www.utexas.edu/data/theft)
[7] [http://www.umich.edu/~policies/ssn-60114.html](http://www.umich.edu/~policies/ssn-60114.html)