

**The Bill Blackwood  
Law Enforcement Management Institute of Texas**

---

---

**The Use of Social Security Numbers as an Identifier  
By Campus Police Agencies**

---

---

**An Administrative Research Paper  
Submitted in Partial Fulfillment  
Required for Graduation from the  
Leadership Command College**

---

---

**By  
Adam W. Trevino**

**University of Texas Health Science Center at San Antonio  
University Police Department  
San Antonio, Texas  
January 2006**

## **ABSTRACT**

The practice of using the United States Social Security Number as an identifier is not uncommon; however it is not a wise practice. In this era of Identity Theft and identity-related crimes, police agencies must ensure they do not unintentionally contribute to the problem. This is especially true of “special entity” police organizations, such as campus police departments, who are regularly involved with the identification and classification of campus community members. In recent years, the social security number has been displayed on university identification cards, parking permits and other documents created or used by campus police departments.

In order to assess the potential and actual impact of campus law enforcement identification practices in Texas, a sample of campus police departments was surveyed and the results were compared against available governmental and media data. Fortunately, the majority of the agencies surveyed who used the Social Security Number as an identifier have recently ceased this practice.

It is concluded that the use of the Social Security Number as an identifier by campus law enforcement agencies has not been a significant contributing factor in the identity-related crimes in Texas. The potential for abuse has diminished significantly within the past five years as a result of campus agencies utilizing alternative numbers.

## TABLE OF CONTENTS

	Page
Abstract	
Introduction. ....	1
Review of Literature . . . . .	3
Methodology . . . . .	7
Findings . . . . .	8
Discussions/Conclusions . . . . .	12
References . . . . .	14

## INTRODUCTION

*Your basic sense of individuality is at stake at this very moment. Who you are and what you stand for can be altered in an instant. Your credit rating, bank account information and criminal records are potentially in the hands of criminals seeking to advance themselves at your expense. You may become the next victim of having your most valuable possession, your identity, stolen. Unless changes are made, organizations using your Social Security Number may be providing the key to a criminal's success.*

In 1936 the Social Security Administration devised a number system to track retirement earnings and tax information for individual Americans. The nine-digit numbering system was designed to positively identify persons even if they shared the same name and date of birth. The use of the Social Security Number as an identifier has become a common practice for many entities throughout the United States. Many organizations took the opportunity to integrate the identification system for their own purposes. There was no specific law governing the use of the numbers until recently. Personal information derived and based upon the Social Security Number became easily available in the private and governmental sectors of business. As a result, criminals took advantage of the situation and began the illegal use of stolen social security numbers or personal identification numbers for personal gain. This is known in today's times as Identity Theft. The results of becoming a victim to identity theft have been devastating and costly for individuals and organizations alike.

As a result of criminal activity associated with the unlawful acquisition and utilization of personal information, the United States Government has conducted studies and implemented legislation aimed at preventing identity theft and prosecuting offenders. Identity theft is the fastest growing crime in America, with Texas ranking fourth in the nation in the number of victims. Law enforcement agencies state-wide

have already felt the impact of this problem. While many departments have been exposed to the topic by taking reports for credit card abuse, forgery and other identity-related offenses, some departments may be contributing to the growth of the problem.

Campus law enforcement agencies are at great risk for liability. Campus police departments are special entity police organizations aimed at providing comprehensive law enforcement and auxiliary services. In providing services such as parking, issuing ID Cards and keys, providing battery boosts or door unlocks as well as other services, many departments utilize the social security number as an identifier.

The use of social security numbers by campus police agencies may contribute to unintended consequences such as identity theft and for potential liability brought about by the victims. The purpose of this report is to provide awareness to campus law enforcement agencies about the problem of identity theft and to encourage using an alternative identifier. Are campus law enforcement agencies putting themselves at risk for litigation without recognizing it? Research will be conducted on publications of the U.S. Congressional committees, independent journals and a survey of Texas campus police agencies. It is anticipated that the results will show the social security number is still being used as an identifier by a majority of campus police agencies even though it may lead to unintended consequences. Campus law enforcement agencies can benefit from this research by developing and implementing an alternative identifier which is cost effective, secure and proprietary to each agency. This will not only protect and benefit the department, but also the campus community it serves.

## REVIEW OF LITERATURE

Since the inception of the use of the social security number, protecting individual privacy has not been a priority. The government encouraged the holder of the number to make it readily available to employers and discouraged persons from applying for or holding more than one social security number. The government was unsure of exactly how many numbers had been issued to each citizen as it was the responsibility of each person to obtain, secure and utilize the number. It was only after many months and in some instances, years of misuse that a holder or the government was aware that the number had been misused.

There were documented misuses of the number for trivial reasons. One instance included an attempt of a wallet manufacturer to demonstrate how easily the social security card fit in the pocket. The model displayed an actual number of a company employee which was misused by over 40,000 people between 1938 and 1977. Another instance involved a woman mistakenly led to believe that her number was one issued by the Social Security Administration. She did not realize she had been using a facsimile number published on a marketing brochure for more than twenty years (US Social Security Administration 2005 [1]).

In some instances, the federal government required the use of the social security numbers as the exclusive numbering system to identify federal employees. Over time, and through executive directives, various government entities were ordered, encouraged or otherwise permitted to use the established numbering system. The Veterans Administration, Civil Service Commission, US Treasury, and the Department of Defense are a few examples of government entities which adopted the social

security number as an identifier (US Social Security Administration 2005 [2]). Local governments and even the private sector began to use the social security number. Inevitably the social security number has become the universally accepted form of identification in the United States. The social security number has become the common form of identification in the consumer arena, from medical services, mortgages, rental agreements, credit worthiness, higher education, etc.... As a result, many entities in the private and public sector began to require the disclosure of the social security number prior to providing goods and services. The number became valuable as some entities began selling it for profit. A number of individuals in society and within the government immediately recognized the danger of using the number universally. The federal government has drafted legislation to prevent the use of the number due to identity theft, credit card abuse, theft and a myriad of other criminal actions involving the abuse and misuse of the social security number (Electronic Privacy Information Center).

Public universities across the country may unintentionally contribute to the growing problem of identity theft, although there is no evidence that the social security number has been compromised and subsequently used to commit fraud (Zeller 2005). Just as Zeller pointed out the potential for breaches of security in the university setting, the University of Connecticut (UConn) recently discovered a hacker software program in its computer system. In fact, UConn notified over 70,000 people that their personal information, including the social security number, may have been illegally accessed over the course of a year (Holtz 2005). According to Grava, the use and storage of the social security number on the university computer server presented the opportunity for hackers and identity-related criminal activity. The faculty, staff, students and vendors

were exposed to the risk of their personal information being compromised. As a result, UConn decided to develop and implement an alternative identifier to prevent future risks (Grava 2005).

Unfortunately, the University of Texas at Austin fell victim to a former student who had hacked into their main-frame computer system. In 2003, Christopher Andrew Phillips hacked into The University's computer system. He had successfully breached the system for over a year, accessing over 45,000 names and social security numbers before the United States Secret Service and university officials caught him. Losses to The University totaled over \$180,000. The U.S. Attorney's Office reported no identity-related crimes had been committed with the information obtained by Phillips because of the swift apprehension by the Secret Service (Sutton 2005).

Despite the Privacy Act of 1974 requiring universities to obtain explicit consent to disclose student information such as the social security number, it has long been misused as an identifier. The problems associated with using the social security number as a university identifier stem from various factors such as the transient status of students, the use of the social security number on the face of identification cards, printing on official transcripts and the tendency of professors to use the number for class purposes such as posting grades. The problem involves not only students, but any member of the campus community. As identified in the case of UConn and the breach of the UT computer system, merely the storage of personal information in the university computer systems poses a risk. According to Gilbert, the University of California at Berkeley and Stanford University have also unintentionally exposed



personal data through the storage of information on vulnerable computers (Gilbert 2005).

This problem is not new. In August of 2004, the University of Toronto experienced the worst web attacks they had ever seen. It took the university officials two days to “sanitize” hundreds of computers only to be hit by another virus shortly thereafter (Acohido & Kessler 2005). These records include personal information on faculty, staff, students and contractors.

Some university officials maintain the philosophy that the individual is ultimately responsible for the protection and security of their social security number. In spite of the potential for abuse, some administrators deem the overhauling of an identification system for universities to be overly costly and unnecessary (Gidjunis 2003). Without federal laws mandating change, there inevitably will be resistance and opposition to making the necessary change.

According to the United States Federal Trade Commission, identity theft is the fastest growing crime in the United States. Texas currently ranks fourth in the nation for identity-related crimes per capita. The cities of Austin, Dallas, Fort Worth, Houston and San Antonio represent the top cities reporting the highest numbers of identity crimes (US Federal Trade Commission 2005).

These cities are home to major universities such as the components of The University of Texas System, Texas A & M, Texas Woman’s University, University of North Texas as well as various private universities and community colleges. Some of these institutions of higher education employ a university police agency responsible for issuing identification cards, parking permits and providing auxiliary services to the

campus community. These police agencies have used and in some cases, may still use the social security number as an identifier.

In light of the growing trend in identity-related crimes and public outcry, the federal government has drafted legislation to prevent the use of the social security number as an identifier. The Identity Theft Protection Act of 2005 serves to prohibit government-wide uniform identifying numbers and prohibits government established identifiers (U.S. Congress H.R. 220 2005). This will reverse the prior policies of the Social Security Administration cooperating with other federal agencies to establish a universal identifier. In addition, The Social Security Number Privacy and Identity Theft Prevention Act of 2005 will prohibit federal, state and local governments from displaying the social security number or any derivative of the number on employee identification cards (U.S. Congress H.R. 1745 2005). The United States Senate is currently working on the "Social Security Misuse Prevention Act" which will prohibit a commercial entity from requiring an individual to provide a social security number when purchasing a commercial good or service (U.S. Congress S.29 2005). At this time, there is no federal law requiring any entity to cease utilizing the social security number as an identifier, there are merely controls as to disclosure of the information.

## **METHODOLOGY**

The author of this research inquired if campus police agencies were using the social security number as an identifier and putting themselves at risk for litigation by victims of identity theft. The author believed that research would show a majority of campus police agencies were using the social security number.

The method of inquiry involved the author researching various news media, governmental press releases and websites as well as publications in the mainstream media.

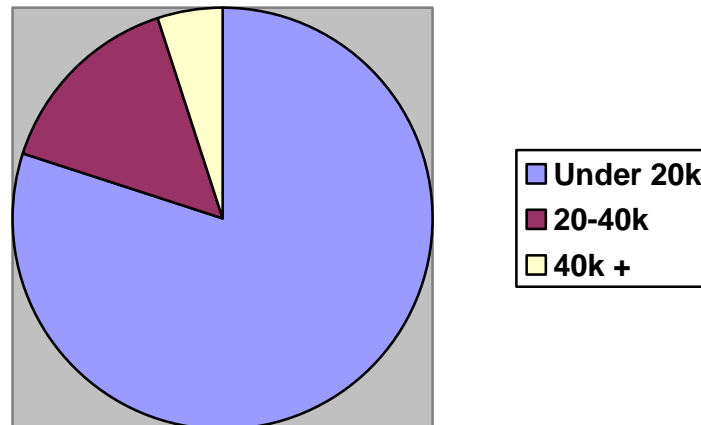
The method of inquiry also included a written survey distributed to campus police agencies of 50 Texas institutions of higher education. The survey sample included various population sizes ranging from a few thousand to tens of thousands of campus community members located across the state of Texas.

The response rate for the survey was 20 out of the 50 distributed or 40%. The data was analyzed to determine if the agency was currently using the social security number as an identifier. The data also provided insight into whether the agency ever used the number in the past, when it ceased using the number and what alternatives may have been developed. Finally, the survey responses provided data on whether identity-related offenses had been reported on the campus.

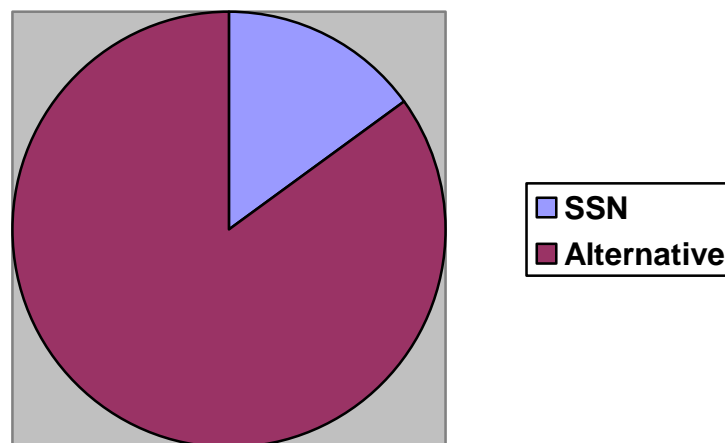
## **FINDINGS**

The author discovered there has been a problem historically with governmental organizations on the federal and state level using the social security number as an identifier. The use of the number as publicly displayed on identification cards, university transcripts, professors' posting of grades using the number or any derivative thereof, etc... has posed a great threat to the individual privacy of campus community members. Additionally, the mere storage of the number in the vulnerable computer systems provided an opportunity and posed a threat from hackers and cyber-criminals obtaining personal data. No data is available to support any actual cases of identity-related offenses involving personal information hacked from university computer files.

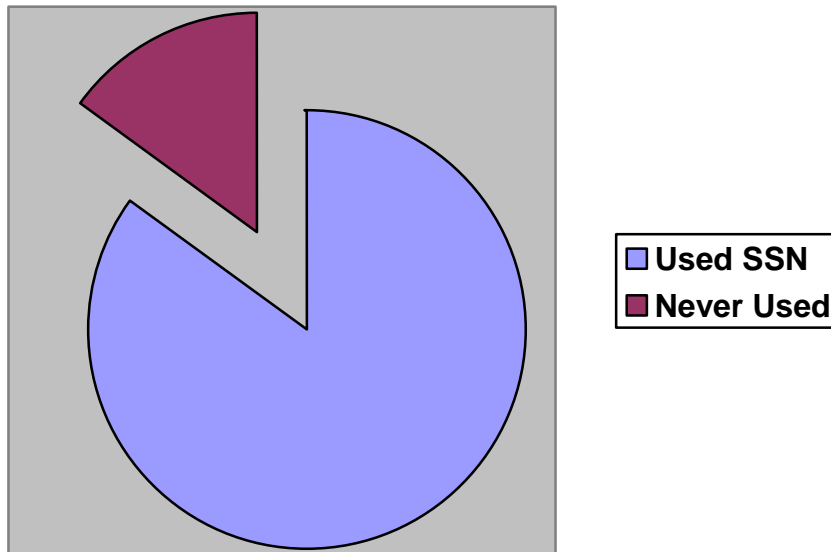
First, the author determined the demographics of the respondents to be primarily campus populations under 20,000. 80% represented campuses with populations under 20,000, 15% represented populations of 20,000-40,000 and 5% represented a population of more than 40,000.



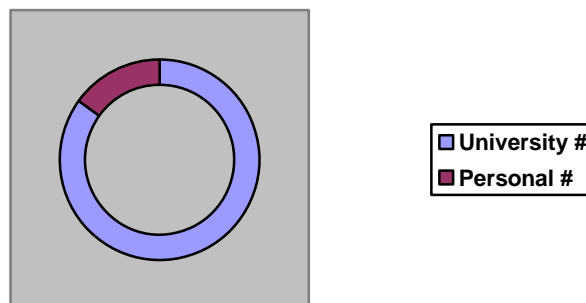
Second, the number of respondents whom currently used the social security number as an identifier was 14%. 86% of respondents use an alternative identifier.



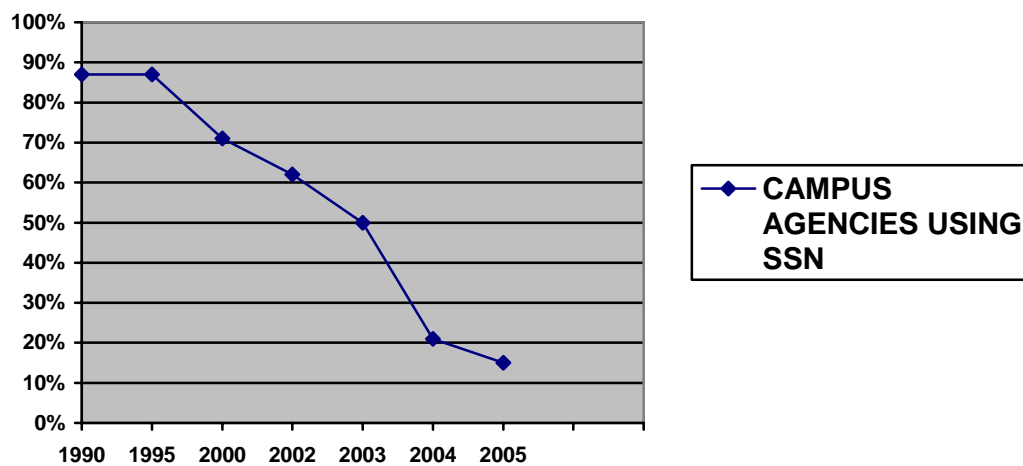
Third, 86% of respondents had at some time in the past used the social security number as an identifier. 14% of respondents have never used the number.



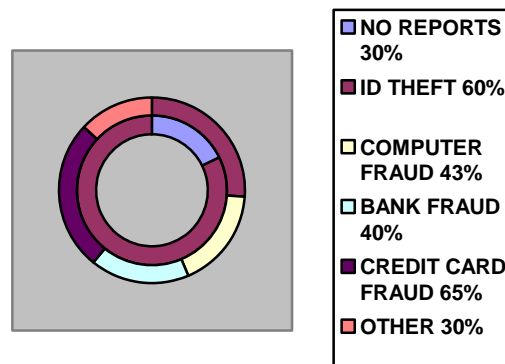
Fourth, some alternative identifiers used by campus law enforcement agencies included a number issued by the university. 86% of campuses reported using such a number. 14% of campuses reported using an alternative identifier such as the driver's license number or personal identification number.



Fifth, regarding the campus police agencies use of the social security number as an identifier, the author was incorrect in his hypothesis. The author believed that the majority of agencies were still using the social security number, however, the survey results indicate the opposite. Only 14% respondents indicated they still used the number. 15% of the agencies never used the number and the other 71% of agencies stopped the practice within the past 5 years.



Finally, 71% of the respondents reported identity-related incidents filed on their campuses to include Identity Theft (60%), Computer Fraud (43%), Bank Fraud/Funds Theft (40%), Credit Card Fraud (65%) and Other employee, student/parent complaints (30%).



## CONCLUSIONS

The purpose of this research was to bring about awareness for campus law enforcement agencies who may use the social security number as an identifier. Considering the contemporary problems and issues revolving around data security and identity-related crimes, the author believed campus law enforcement agencies may unintentionally provide the opportunity for criminals to commit offenses.

The author of this research believed that surveys distributed to campus law enforcement agencies would reveal the use of the social security number may have been or was currently being used as an identifier. The author was not completely correct in his hypothesis. A majority of the police agencies have used the social security as an identifier at some time in the past; however the majority of respondents have discontinued the practice within the past five years. While there was contemporary literature which referred to the potential for privacy breaches through vulnerable university computer systems storing personal data, there has not been any evidence to support the notion that such opportunities resulted in actual identity-related offenses.

The author recognized two limitations of this study. First, the survey sample was limited geographically to Texas colleges and universities. It is possible that the Texas institutions of higher education decided to develop alternative identifiers in light of the increasing awareness of identity-related offenses. Second, it may be unlikely to accurately determine whether or not a person has become a victim of identity-related crimes due to the university police agencies' practice of using the social security

number as an identifier. In most cases, victims do not realize they have become victims until several months after their identity has been stolen or misused.

The relevance to law enforcement in this study hinges upon the premise that the use of social security numbers by campus police agencies has existed and in some cases still exists. In order to prevent identity-related crimes from occurring, the campus police agencies must continue to find other methods of identifying faculty, staff, students and other members of the campus community.



## REFERENCES

- Acohido, Byron & Kessler, Michelle (2004, August 26). Worm, virus threat grows: Attacks expected to get worse, could even bring Net to its knees. *USA Today*, pp. 3B.
- Gidjunis, Joseph (2003). *Social Security Number Use Puts Students At Risk*. Retrieved July 16, 2005, from [http://www.youngmoney.com/consumer/consumer\\_fraud/030205\\_03](http://www.youngmoney.com/consumer/consumer_fraud/030205_03).
- Gilbert, Alorie (2005, July 26). Survey: ID theft hard to shake off. Retrieved July 26, 2005, from [http://www.nytimes.com/cnet/CNET\\_2100-1029\\_3-5805671.html](http://www.nytimes.com/cnet/CNET_2100-1029_3-5805671.html).
- Grava, Karen A. (2005, June 24). *UConn server may have been breached*. Retrieved September 12, 2005 from <http://www.uconn.edu/newsmedia/2005/june05/rel05049.html>.
- Holtz, Jeff (2005, July 5). In brief; UConn finds breach in computer system. *The New York Times*, Late Edition-Final, Section 14CN, Page 2, Column 6.
- Sutton, Johnny (2005, September 6). *Former Student Sentenced For Hacking Into U.T. Computer System*. Retrieved November 18, 2005 from message posted to [http://www.usdoj.gov/usao/txw/press\\_releases](http://www.usdoj.gov/usao/txw/press_releases).
- Zeller, Tom (2005, April 4). Some Colleges Falling Short On Data Security. *The New York Times*, Late Edition-Final, Section C, Page 1, Column 5.
- Electronic Privacy Information Center (2004, September 28). Social Security Numbers. Retrieved July 17, 2005, from <http://www.epic.org/privacy/ssn/default.html>.
- U.S. Congress H.R. 220 (2005). House Resolution 220. *Identity Theft Prevention Act of 2005*. Retrieved November 20, 2005 from <http://thomas.loc.gov/cgi-bin/thomas>.
- U.S. Congress H.R. 1745 (2005). House Resolution 1745. *Social Security Number Privacy and Identity Theft Prevention Act of 2005*. Retrieved November 20, 2005 from <http://thomas.loc.gov/cgi-bin/thomas>.

U.S. Congress S.29 (2005). Senate Bill 29. *Social Security Number Misuse Prevention Act*.

Retrieved November 20, 2005 from <http://thomas.loc.gov/cgi-bin/thomas>.

U.S. Federal Trade Commission (2004). *Identity Theft Victim Complaint Data: Figures and*

*Trends in Texas*. Retrieved July 16, 2005, from

<http://www.consumer.gov/idtheft/cy2004/texas%20yc2004.pdf>.

U.S. Social Security Administration (2005) [1]. *Social Security Numbers: Social Security Cards*

*Issued by Woolsworth*. Retrieved July 16, 2005, from

<http://www.ssa.gov/history/ssn/misused.html>.

U.S. Social Security Administration (2005) [2]. *Social Security Numbers: Social Security*

*Number Chronology*. Retrieved July 16, 2005, from

<http://www.ssa.gov/history/ssn/ssnchron.html>.