

Oracle's SSN Vault

An Oracle White Paper
May 2007

DATA BREACHES IN HIGHER EDUCATION

University of California, San Francisco: April 2007. 46,000 names, SSNs, and bank account numbers potentially compromised.

City College of San Francisco: February 2007. Names, grades, and SSNs of 11,000 students posted on unprotected web site.

East Carolina University: February 2007. A programming error exposed personal information of 65,000 students, alumni, and staff on the university's web site.

University of Idaho: January 2007. 70,000 names, addresses, and SSNs and 300,000 other personal records exposed after theft of three desktop computers.

University of Colorado: December 2006. 17,000 names and SSNs of people attending orientation sessions between 2002 and 2004 exposed.

University of California, Los Angeles: December 2006. 800,000 names and personal information from students, parents, and faculty exposed.

—PrivacyRights.Org

EXECUTIVE OVERVIEW

The purpose of this document is to facilitate an understanding of Oracle's Secure Social Security Number (SSN) Vault, a solution that allows higher education institutions to centralize and protect sensitive data like personally identifiable information (PII) such as the SSN.

Although the SSN has been in wide use as a personal identifier for a number of years, recent concerns about identity theft have forced institutions and governments to restrict its usage in information systems. In part because they often have open systems and broad access to a wide variety of users, higher education institutions have been subject to many security breaches exposing PII data of millions of individuals in recent years. Modifying internal information systems to replace the SSN as a personal identifier is an expensive and time-consuming proposition; similarly attempting to secure sensitive data via policies and procedures is difficult within a higher education environment due to its open and decentralized requirements. Oracle has developed the Secure SSN Vault solution to allow institutions to better protect sensitive data like the SSN and other PII and to enable the institution to cease using the SSN as a personal identifier without modifying internal applications.

INTRODUCTION

Security and regulatory requirements have surpassed most applications' ability to secure sensitive data appropriately and the institutions' ability to maintain this level of security and compliance. To illustrate this, in August 2006, a cover story in *USA Today*¹ reported that since January 2005, at least 109 publicly disclosed breaches occurred at 76 schools and that colleges and universities were responsible for one-third to one-half of all PII breaches within the United States. In that same year, Educause ranked security and identity management as the number one issue facing higher education institutions.²

Due to increasing concerns over identity theft and protection of privacy rights required by regulations, higher education institutions in the United States are exploring ways to limit the use and visibility of PII and in particular, individuals' SSNs. Because of the ongoing challenge to protect and secure the SSN and other PII within higher education, Oracle is working to provide enhanced protection for sensitive information through a strategy called "Secure SSN Vault." This paper describes the Oracle Secure SSN Vault strategy that employs Oracle middleware products to intercept SSNs entering and exiting internal systems and replace them

with non-PII data, while still allowing the actual SSN to be provided for external entities that require it.

PROTECTING AND SECURING PII

What is PII? In general, PII is data that information systems use to identify a particular individual. Examples include:

- Name
- SSN
- Drivers license number
- Home address
- Phone number
- Passport/VISA number
- Credit card number(s).

“In 1936, the Social Security Administration established the Social Security Number (SSN) to track workers’ earnings for Social Security benefit purposes. Despite its narrowly intended purpose, the SSN is now used for a myriad of non-Social Security purposes. Today, SSNs are used, in part, as identity verification tools for services such as child support collections, law enforcement enhancements, and issuing credit to individuals. Although these uses can be beneficial to the public, the SSN is now a key piece of information in creating false identities. The aggregation of personal information, such as SSNs, in large corporate databases and the increased availability of information via the Internet may provide criminals the opportunities to commit identity theft.”

**—Barbara D. Bovbjerg, Director,
Education, Workforce, and Income
Security Issues, US General Accounting
Office, Publication GAO-05-1016T, Sept 15,
2005**

Of all PII data, the SSN is the most challenging data to secure and protect as well as the most valuable to an individual. Though never intended to be a “national ID,” the SSN was used for many years by most information systems as the unique identifier of choice for an individual. And although its use has been discouraged and more recently restricted by privacy compliance regulations, it is still widely used: the United States government identifies individuals primarily through the use of SSNs. Income taxes, Social Security, Medicaid, transcripts, investments, insurance, driving records, and criminal records are all usually correlated to the SSN. Longitudinal studies can also be based off of SSN information. Therefore, it is imperative that an institution be able to utilize SSN information for communication with external parties and yet have the ability to verify uniqueness within an institution. The Oracle Secure SSN Vault provides this capability, which is what distinguishes it from other unique IDs that an institution may be already utilizing.

HIGHER EDUCATION CHALLENGES

Higher education institutions face an enormous challenge in protecting and securing PII information because of their unique need to collect an immense amount of PII information for various purposes. These include:

- Student systems, Housing, Parking, Library, Medical, Alumni, Research,
- Departments, Student Data, University Police, University/State Auditors,
- General Counsel, Student Health Services, Counseling Center,
- Veteran’s Service, Health Science Center, Decision Support,
- University Advancement (Alumni), Athletics, Registrar
- ROTC (Air Force, Army, Navy), Continuing Education
- Financial Aid, Admissions, Graduate School, IT
- State and Federal agencies, Student and Exchange Visitor Information System (SEVIS)

Further, colleges and universities have unique challenges related to their heterogeneous user base. Unlike corporations that can dictate data security policies and procedures to employees, higher education institutions must deal with the differing needs (and enforcement capabilities) of a widely diverse user population. From staff to faculty, to researchers, to students, the amount of control the institution is able to enforce varies widely: policies and procedures can be tightly enforced for staff, just as they are in corporate environments, but policies and procedures can be difficult to enforce among faculty (especially tenured faculty) and next to impossible to enforce with students, who often tend to think of their university as a glorified internet service provider (ISP).

Why are higher education institutions so often targeted for identity theft? There are several reasons: thousands of new identities are created each year; information is usually of high quality; and university systems are often not difficult to access, since they may have limited budgets for data security.

These challenges have resulted in a “target-rich” environment for obtaining PII data. In 2006, a survey of 192 higher education institutions found that 58 percent reported a security breach and 33 percent reported a data loss or theft². This can also be extremely costly to a higher education environment as well. *The Chronicle of Higher Education* cited that the direct cost for each identity breached was approximately \$10³. Depending on the circumstances of the loss, the estimate can be even higher: between \$50 and \$250 per identity⁴. Class action lawsuits have also been filed after breaches occurring within higher education, further adding to potential costs.

In addition to the direct costs, other ramifications can exist: Many higher education institutions have removed chief information officers and executives from their positions due to breaches occurring within their respective institutions. Additionally, higher education institutions may have difficulty attracting researchers. Dr. Joanne Logan, a researcher at the University of Tennessee, cited security as one of 10 factors that researchers consider when determining institutions with whom they will conduct their research. And, finally, higher education institutions may lose critical funding for research initiatives.

Breaches are not limited to those caused by hackers, theft, or other malicious activities. In 2006, 21 percent of breaches in higher education occurred due to “human/software incompetence⁵,” such as someone leaving a printout or USB drive with sensitive information in a public place or a developer causing programming errors that inadvertently posted sensitive information to public web sites. In fact, a common theme that is heard within higher education is, “Help protect us from ourselves.”

PROTECTING PII

Clearly, protecting PII is a major concern in higher education, as it is elsewhere. In the past, many higher education institutions have spent an immense amount of time and effort trying to protect PII—such as the SSN—with the use of security policies and procedures. These policies and procedures address how such information can be used, its proper disposal, its allowable dissemination, access, encryption, storage methods, and so on. This is a costly and time-consuming process. Further, as mentioned earlier, the heterogeneous nature of the user

environment makes it effectively impossible to enforce these security policies adequately.

Once SSN data exists within all of the “core” application systems (i.e., student, human resources, and financial), it becomes subject to the security that is implemented within each of the applications that use it—which may be inconsistent at best and non-existent at worst. SSN and other PII are also then disseminated to various departmental and personal systems, some of which are centrally controlled and some of which the institution may not even be aware. In this type of environment, the SSN is communicated to and stored in dozens of places in university systems and may find its way into untold numbers of departmental systems, documents, and spreadsheets. Given the sheer volume of replication of the SSN, remediating the risk of breaches from all the known and unknown points of exposure has proven impossible. This also makes maintenance of the systems and data difficult (and expensive) as the institution’s processes, users, and applications change over time.

So the real question becomes: Why not just eliminate SSNs within the higher education environment? Outright elimination of the SSNs from all higher education systems is simply not possible—they are required by too many critical applications. If the institution employs an individual, the SSN is required to be able to collect and report tax, retirement, and medical information to federal and state governments. Further, the SSN is required for any individuals for whom background checks may be run, such as security personnel, health care personnel, or even simply faculty and staff. The SSN is also required for most financial accounting applications such as grants and financial aid and for the Student and Exchange Visitor Information System (SEVIS) that tracks students, exchange visitors, and their dependents. The SSN is also needed to match individuals to their information in external systems, often only possible through the use of the SSN.

In addition to being mandatory for many applications, a unique personal identifier, such as the SSN, accurately identifies an individual for all the institutional systems with which they interact for reporting purposes, such as: Parking, Library, Alumni, Athletics, Healthcare, Research, etc.

faculty, students, and staff), e.g., those who participate in non-course programs such as summer camps and volunteer efforts, as well as guest speakers, vendors, and others who may need temporary access to some of the university’s facilities.

SOLUTION: ORACLE SECURE SSN VAULT

Because of wide use both inside and outside the institution, elimination of the SSN as an identifier for an individual is simply not possible. Furthermore, policies and procedures provide inadequate protection in a higher education environment. So how is it possible to protect the SSN and other PII data when they are used in so many different systems? Oracle’s answer: Secure SSN Vault.

As Figure 1 illustrates, the Secure SSN Vault solution by Oracle is a three-part strategy. Part One is to capture real SSNs (and potentially other PII data) from

Securing personally identifiable information (PII) such as the SSN in one location is feasible and relatively simple: securing duplicates of that information spread out over multiple application systems is practically impossible.

SSN providers (such as students, faculty, and staff) upon entry in the university’s systems. An “Alternate ID” (AltID) or “fake SSN” (that is a unique nine-digit number for an individual and that has the same format as a real SSN) replaces the captured SSNs. The AltID is then passed to university systems as if it is the true SSN, and internal applications use it as they would a true SSN.

Part Two of the strategy is to encrypt the true SSN and store it in one centralized database. This “Secure SSN Vault” uses leading practices’ defensive in-depth technologies (e.g., encryption, auditing, authentication, and rules) to provide maximum protection of the data. Defensive in-depth technologies prevent dissemination of SSN information within the various applications while allowing them to operate as they would normally.

Part Three of the strategy is to capture AltIDs as they are transmitted outside of university systems, transform them back into true SSNs, and transmit the data to legitimate SSN recipients (i.e., federal and state governments and other legitimate users) in a secure form.

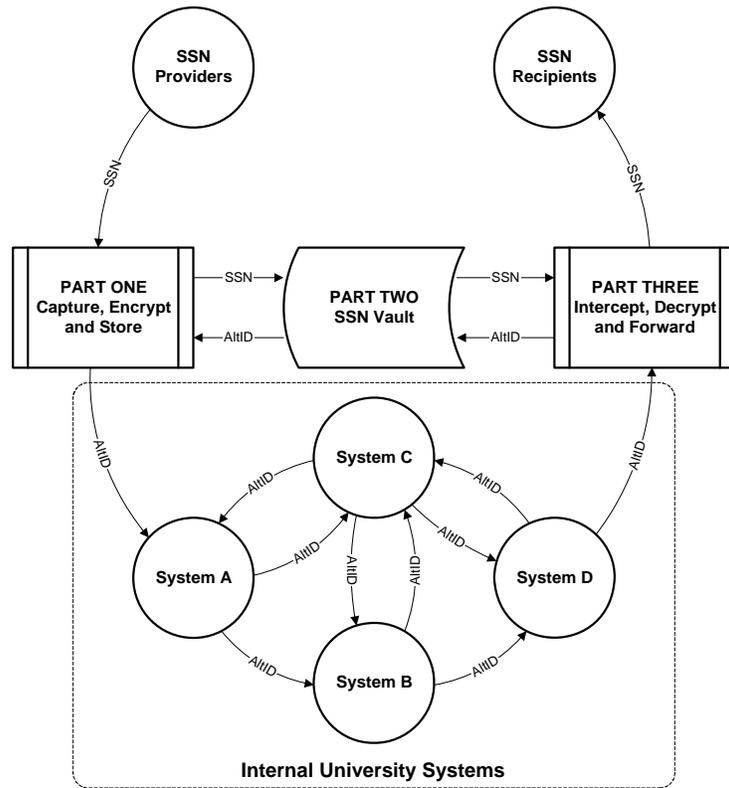


Figure 1: Secure SSN Vault

The SSN and PII data are centralized in a single location inside the Secure SSN Vault and with an adequate level of encryption that allows for exemption from state and federal privacy notification regulations. In other words, if any of the AltIDs are accidentally or maliciously exposed, there is no “breach,” since no actual PII data has been exposed. The AltIDs are completely meaningless outside the context of the university systems. Because the AltID has the same nine-digit numeric

At one Oracle higher education customer that had already undertaken a major project to remove SSNs from the systems, SSNs were found to be remaining in at least 18 application systems.

format as actual SSNs, modifications to university systems are unnecessary, as applications utilize the AltID as if it were a true SSN.

Web services are utilized in Part One of the solution, so that once an identity is created within the SSN Vault, Web service rules enable the dissemination of the AltID to all the appropriate application systems. (Unlike the simplified schematic in Figure 1, the AltID would be supplied to all of the university systems that would formerly use the true SSN as a data source). This AltID will enable users of the applications to confirm that they are working on the appropriate individual's information without having to bear the responsibility of utilizing the SSN to verify this. Once applications generate reports that require SSN information, a Web service authenticates the report in Part Three of the solution and then routes it through a Web service for transformation and secure forwarding.

The centralization of the solution allows for security policies and procedures around this data to be easy to enforce and adherence to them easy to monitor. Authorized university personnel are then able to perform extensive auditing on this centralized database, along with exclusive authentication regarding access to data. Further, the institution can customize alerts to provide proactive detection of improper use of data.

Rules that limit which SSNs will be unencrypted depending upon the report/person accessing them can also be utilized (e.g., student SSNs would not be allowed to be unencrypted by a W-2 report if the student had never had an employee status with the institution). Since all SSN data is now centralized, the institution greatly minimizes the possibility of the SSN being breached with a lost or stolen asset.

And, in case of a compromise, the Secure SSN Vault uses the Oracle Advanced Security Option, which allows for the storing of the encryption algorithm on a separate server so that if the physical server were ever compromised, the encryption algorithm would not be. Database administrators are able to maintain this database but prevented from viewing the non-encrypted data thus further minimizing risk.

Finally, by utilizing the AltID in place of the true SSN, the higher education institution can still fulfill its state and federal reporting requirements, as well as track an individual's interaction with the institution without bearing the risk of exposing the SSN information. The Oracle Secure SSN Vault provides for most institutions to be relieved from state and federal privacy notifications regulatory requirements because the sensitive data is stored and transmitted in an encrypted format.

ADDITIONAL ADVANTAGE: EXPOSING "SHADOW" SYSTEMS

Centralizing the storage of SSNs and using AltIDs in their place in internal systems has an additional beneficial by-product: a tendency to expose so-called "shadow" or rogue systems. As every organization knows, end users have a habit of creating their own applications outside of the centralized or controlled IT environment. Often, dozens to perhaps hundreds of these home-built applications exist at an institution; using spreadsheets or personal databases, end users have built these

shadow systems so that a few individuals can use them to perform some specialized function. As these systems pull data from officially sanctioned systems, they often contain copies of PII data, such as the SSN. Most organizations have no idea how many such systems exist and no practical way of tracking them.

The use of Secure SSN Vault can often drive these shadow systems into the open. Once Secure SSN Vault has been implemented for all the centrally controlled or “official” internal systems, shadow systems that pull information will start pulling AltIDs instead of SSNs. If the SSN has any meaningful usage in the shadow system, end users will notice immediately that the SSNs have changed (or no longer function), which then forces them to communicate with central IT for support. At this point, the determination can be made whether or not the end user has a legitimate need for SSNs or if AltIDs can work as personal identifiers in their systems as well. If the need is legitimate, the shadow system can be incorporated into the Secure SSN Vault strategy.

MAINTENANCE

The Secure SSN Vault solution is built using off-the-shelf Web service technologies. These technologies ease the level of effort in creating and maintaining interfaces with the institution’s applications. Since the institution’s applications will require little to no customizations, ongoing maintenance of these applications should not be affected. Moreover, the institution can perform authentication of the Web services against existing identity management repositories.

FUTURE OPPORTUNITIES

Higher educational institutions can also utilize additional Web services to improve the effectiveness of identity management against the Secure SSN Vault. For example, a Web service could be set up to validate identities with the Social Security Administration, further confirming that people not only provided a legitimate SSN, but also that the SSN provided is actually theirs. This would aid in further minimizing duplicate identities and match/merge efforts. Another possible Web service would be one that validates SSNs with government tracking databases, such as those from Homeland Security, to verify that only valid contractors are being utilized. Finally, Web services adapters for applications can also be shared among higher education institutions, making the entire community more secure and providing additional sources of intellectual capital.

Additional benefits to obtaining a single source of truth for identities exist. Integrating identity data will now be much easier, since applications and systems are feeding from the same PII repository. Further, adhering to regulatory requirements such as HIPAA and FERPA will be simplified due to the limited amount of identity data that is now needed within the applications.

CONCLUSION

Protecting and securing PII data such as the SSN is the biggest data security problem facing higher education institutions today. Breaches of sensitive data,

SSNs aren't the only candidates for storage in the SSN Vault. Any personally identifiable data such as biometric information, bank account numbers, challenge/response authenticators, and so on can be stored in encrypted form.

both inadvertent and malicious, have been numerous over the past few years and have been increasing both in frequency and in magnitude. Protecting PII data by policy and procedure is an expensive and virtually unworkable solution in a university environment. Many institutions are working to drive SSN information out of applications in which it is not absolutely necessary. However, this may impede vital reporting and analysis due to the inability to guarantee uniqueness for an individual. Many institutions have moved to not using SSN as a unique identifier within their Student system but the SSN data is still present within these applications for external reporting. The Oracle Secure SSN Vault allows for institutions to keep their existing student and employee IDs while still providing a unique number across all applications without the privacy exposure of SSNs. Centralizing SSNs and other information in a Secure SSN Vault and using Web services to capture and convert incoming and outgoing SSNs into Alternate IDs is a viable and economical solution to a complex problem.

REFERENCES

- ¹ Mary Beth Marklein, "Colleges are Textbook Cases of Cybersecurity Breaches," August 1, 2006, http://www.usatoday.com/tech/news/computersecurity/hacking/2006-08-01-college-hack_x.htm
- ² "Top-Ten IT Issues, 2006," May/June 2006, Educause Review
- ³ John Moore, "Most Campuses Report Security Breaches," October 10, 2006, FCW.com, <http://www.fcw.com/article96412-10-10-06-Web&printLayout>
- ⁴ Andrea L. Foster, "Worried About Hackers? Buy Some Insurance," *The Chronicle of Higher Education*, October 13, 2006, <http://chronicle.com/weekly/v53/i08/08a04101.htm>
- ⁵ Khalid Kark, "The Cost of Data Breaches: Looking at the Hard Numbers," SearchSecurity.com, March 21, 2007, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1248216,00.html
- ⁶ PrivacyRights.org, <http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm>



Oracle's Secure SSN Vault

May 2007

Author: Ted Sherrill IV

Contributing Authors: Dave Higgins, Richard Schad

Oracle Corporation

World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

oracle.com

Copyright © 2007, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.