

Written Testimony of Jim Davis
Associate Vice Chancellor, Information Technology
Chief Information Officer
Professor of Chemical Engineering
University of California, Los Angeles
Before the Subcommittee on
Terrorism, Technology and Homeland Security
Committee on the Judiciary
United States Senate

Identity Theft: Innovative Solutions for an Evolving Problem

March 21, 2007

Lessons Learned from Notification of a Large Breach

Madam Chairwoman, Ranking Member Kyl, Members of the Committee, I appreciate this opportunity to appear before the subcommittee. Last year, UCLA was the victim of a large database security breach. More than 800,000 people were notified that their Social Security numbers might have been illegally accessed. The scale and complexity of the breach amplified the tension of competing goals raised in decision-making and resulted in a number of important lessons learned about responding to an incident of such magnitude: deciding whom to notify when computer forensics are inconclusive, the logistics of a large-scale notification and how notification aligns with our high respect for individual privacy. I would like to share some of these lessons with you today.

Computer forensics uncovered evidence that significantly confirmed only a small percentage of the 800,000 individuals in our database had their Social Security numbers accessed and needed notification under California law. The campus then faced a difficult decision about whether to notify the vast remainder of potentially affected individuals in the absence of significant confirming technical evidence. We were acutely aware of the large impact our

decision would have on the individuals and on our campus. What was the campus's position on notifying these individuals?

A clear consensus quickly emerged that UCLA wanted to do the right thing, even if it caused negative repercussions for the campus. Providing possibly broader notification than was strictly legally required was part of this position. Individual privacy is a cultural and institutional value highly regarded by the University of California and we felt notification supported this value, both as events were unfolding and subsequently during discussion of the security breach with our Advisory Board on Privacy and Data Protection.

At the same time, UCLA itself felt victimized. UCLA had taken significant technical, administrative and physical security measures to protect its sensitive data, yet it still suffered this sophisticated attack. Not only did the attack potentially affect individuals in the database, but the University made extensive efforts to assess and remediate the situation, with many staff spending night and day for several weeks working to handle the breach.

The Breach

The restricted UCLA database contains certain information on all current and some former students, faculty and staff, as well as some student applicants and some parents of students or applicants who applied for financial aid. It also includes information about all current and some former employees at the University of California Office of the President and at the University of California, Merced (for which UCLA does administrative processing). In all, information for some 803,000 persons was stored in this database, including names, Social Security numbers, dates of birth, home addresses and other contact information. It did not contain drivers license, credit card or banking information.

The FBI set up a mechanism to take reports of alleged identity theft believed to be due to this breach through their Internet Crime Complaint Center. To date, UCLA has not received any information, either directly or from the FBI, to suggest that the compromised data has been used illegally.

UCLA computer system administrators first discovered the breach on November 21, 2006, when they noticed unusually high volumes of activity on a campus data server. Further investigation indicated that an attack was in progress, and security staff took the compromised system off the network and began a computer forensics investigation.

The University of California's Electronic Information Security policy includes guidelines for uniform handling and reporting of security breaches under the California law. UCLA's well-established security incident response process was invoked, and the FBI was alerted and began conducting its own investigation. Having an incident response protocol defined in advance was critical to mounting a prompt and effective response to our security breach. While we strive for a zero incident target with respect to security, we remain prepared for the worst, a position consistent with the guidebook on Protecting Personal Information just issued by the Federal Trade Commission ("Plan Ahead" is the last step of its five-step program.)

UCLA's systems were in full compliance with University of California (UC) and campus policy governing security standards and practices, but system log analysis showed that sophisticated and malicious attackers were able to exploit an undetected flaw in one of its applications. It was particularly disturbing to find that our systems were being attacked by a criminal with clear intent to collect Social Security numbers, unlike many other breaches

reported in the press and by other UC institutions where the data was not the target – e.g., missing laptops or servers compromised for illegal music and movie file sharing.

Forensic analysis continued in the days following the initial discovery. Conducted in cooperation with the FBI, this analysis revealed organization, sophistication and a multiplicity of attack modalities that were not originally evident. Because of the sophisticated nature of the attack, the hacker was able to conceal his or her activity or make it blend in with legitimate activity, allowing the illegal access to remain undetected for a little more than a year before it was discovered in November 2006.

Whom to Notify?

By campus policy, the final decision to notify and the extent of notification rests with the chief information officer. We assembled the equivalent of an outside, objective notification review team that included the chief information officer, the UCLA directors of information technology security and information technology policy, legal counsel and the director of information technology policy for the University of California system.

In our deliberations, we faced a fundamental tension between speed and accuracy in determining whom to notify during the ongoing forensic analysis. We wanted to let potentially affected individuals know as soon as possible about the breach so they could take action by placing a fraud alert or a credit freeze; however, the complexity of the forensics meant new findings occurred almost daily, and the size of the potentially affected population changed significantly with these new findings. We did not wish to alarm and inconvenience hundreds of thousands of people if there was no reason to do so, or to send out multiple potentially conflicting notices. Woven throughout our deliberations was what the California

Law About Notification in Instances of Security Breaches (California Civil Code, §1798.29) required in the absence of positive proof.

Initial results of our computer forensics indicated a relatively small population whose data could have been acquired. Subsequent results indicated the possibility of access to the full database of 800,000; however, continued analysis led us to believe the attack was targeted only on the smaller segment of the database. In our deliberations we felt a strict interpretation of the State notification law (“...shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person”) would require us to notify only this smaller subset.

In the absence of positive proof about whether the vast majority of people’s information had actually been acquired, we used a set of criteria articulated by the University of California in 2003 – based on the California Office of Privacy Protection’s recommended practices – to help think through exactly such ambiguous situations. Among other things, we considered the duration of the exposure and indications that the attack specifically sought personal information, whether we had any definitive evidence that the information was *not* acquired, as well as the potential harm to individuals if the wrong decisions were made. (These criteria have since been expanded upon by the EDUCAUSE/Internet2 Security Task Force, as part of their Data Incident Notification Toolkit.)

Careful consideration of all factors ultimately convinced us to notify the largest group, even without a legal requirement or evidence of acquisition. Underlying this decision was an ethical responsibility to protect against potential fraud and a high regard for the privacy of

individuals. Our goal was then to rapidly reach as many of the 800,000 people in the breached database as possible.

The Logistics of Notification

The specter of identity theft raises anxiety and anger, and we did not want to compound the situation by being ill prepared to address individuals' concerns once our notification began. As with other institutions, we deemed it essential to establish a call center and Web site prior to notification. Since we also wanted to minimize delay, our strategy was to get our base communications structure in place as quickly as possible, begin the notification process and then continually make needed adjustments as we monitored results. In tandem with our deliberations about whom to notify, the incident response team, including University Communications, built an identity alert Web site with information about the breach, what individuals could do to protect themselves from identity theft and the latest news from UCLA and the FBI. We also developed critical information to provide to the staff that would be answering phone calls from affected individuals. Finally, a call with the California Office of Privacy Protection provided several thoughts, including a recommendation to inform the three credit reporting agencies about our breach and our large notification process, which we did.

Institutions we spoke with told us to expect a 3% call rate, which translated into about 25,000 calls. Immediately, making arrangements to outsource call center operations was not just on the critical path to notification, but became the critical path: we had never had to do this before, and finding a suitable call center vendor and completing a contract on an expedited basis became mission critical.

Notification began on December 12, 2006, the earliest date possible after determining the scope of the incident, setting up arrangements to communicate with 800,000 people and being prepared to handle the huge volume of anticipated telephone calls. University of California guidelines require us to employ written hard copy or email notice, or in cases where sufficient contact information is not available, substitute a notice via prominent display on the campus Web site for a period of at least 45 days.

Our notification process was a coordinated effort involving e-mail, U.S. mail, the news media and our Web site. Letters were sent by email or U.S. mail to the approximately 70% of individuals for whom we had addresses. (UCLA's policy mandates attempted notification of all affected individuals, not only California residents as required by State law.) We issued a news release, and on the same day we placed a story in the Los Angeles Times, which led to stories in print and broadcast outlets across the country and internationally. All communications pointed to our toll-free number and Web site. Our statistics demonstrate success in reaching approximately 75-80% of the affected database population.

We received 12,000 calls the first day. At its height, the call center operation included 1,600 (non-dedicated) operators at 26 locations, handling as many as 1,000 calls per hour. To date, the hotline has received almost 36,000 calls (about 4.5% of those notified) and though now scaled back, it is still accepting calls. Operators were able to confirm that a caller was in the affected database and provide basic information about fraud alerts and credit freezes, or escalate calls to a higher-level official. They were specifically instructed to use a sympathetic tone. The statistics and feedback provided by the call center vendor were reviewed at the end of each day and used to revise and fine tune our approach and the information used by operators. For example, we heard early on that some recipients read our notification letter to

mean that their identities had, in fact, already been stolen and we modified the call center responses to correct this misunderstanding.

We found three groups of callers: the largest group felt violated and anxious and wanted the connection with a live person for answers, reassurance, clarification and empathy; a much smaller group just wanted information; and something under 2% of callers were sufficiently angered or distraught that they demanded to speak with a higher-level UCLA official. Our escalation process designated an individual who had the right combination of knowledge, sympathy and ability to ensure follow-up action to provide a return call to each such caller. Of the 600 or so callers who spoke with this individual, we had five people who remained dissatisfied.

Our Web site was a vital component of the notification process. We continued to develop and add content as new information became available that would expand its capacity to inform affected individuals. For example, we had initially relied on the credit reporting agencies' Web sites for information about placing a fraud alert. However, we received reports from callers that the procedures deviated from those described on their Web sites and so we had staff call the agencies to get specific details that was then detailed on our identity alert site. To date our Web site has received almost 105,000 unique visitors, with an average of 15,000 daily visitors during the first week following our announcements.

On January 10, 2007, a second letter was sent to approximately 28,500 individuals and posted on the identity alert Web site. By this point, our forensic analysis indicated that these were the only people for whom we had significant evidence that their Social Security numbers had actually been acquired. There remained no conclusive proof of access to the rest of the database.

Lessons Learned

We offer six actions to consider in being prepared for and in responding to a breach.

1. Convene an independent and objective panel for deliberations about whom to notify. A complex technical environment required ongoing forensic investigation to understand modes of attack, presumed intent and our belief about the degree to which the hackers had the ability to carry out this intent. Faced with rapidly shifting information, the administrative panel of experts convened was key to determining compliance with applicable California law and in judging the competing factors in notifying the large majority of individuals for whom we had no conclusive proof. We continue to believe our decision was the most suitable; but notification did cause concern and inconvenience, the drawback in notifying when the risk of harm is at best unclear.

2. Make provisions for confidentiality. As the forensics investigation continued and we were still learning about the nature and extent of the attack, we were keenly aware of the need to protect our systems from further harm to the extent possible. Maintaining confidentiality during this “learning” stage was pivotal to doing so. Concerns about confidentiality were also threaded throughout our efforts to share information with others who could have benefited from our experience, in terms of information going out prematurely that would have adversely impacted the effectiveness of our notification.

3. Ensure that the call center and Web site are ready to go when notification occurs. Given the enormous volume of callers and visitors to our Web site, without these channels of information reinforcing each other, confusion and frustration levels would surely have been much higher.

4. Notify using different channels. We preferred individual notification – email and U.S. mail – but to ensure that the affected population learned of the breach, the toll-free number and

our identity alert Web site, we also used our UCLA's home page and the media. We believe all channels we used were important: email and the media for the fastest way to reach individuals and U.S. mail for a more personalized notice. We did receive callers who expressed annoyance about not having received a personal letter or email and "only" hearing about the breach through the media, but we felt our goal of awareness had been achieved.

(When we heard complaints about the lack of personalization – specifically, the use of "Dear Friend" as a salutation in our first letter – we took pains to ensure that the second group of letters was personalized with the individual's name clearly shown in a windowed envelope.)

5. Offer access to solid information through different channels and keep track of how they are used. It was important to be able to give useful and accurate information, such as the specifics on how to protect oneself from identity theft, how a fraud alert works, how a credit freeze differs from a fraud alert and how to implement them. We spent effort researching this information and tested the methods ourselves. Offering this information through both the identity alert Web site and the call center was important: individuals without a computer were unable to easily access our Web site; callers who demanded escalation from an operator often did not wish to go to the Web site; and with the volume of visitors to our Web site, doubtless many who went to the Web site to get information did not have to call. Finally, all of the statistics we kept on these communications methods have helped us to understand how successful we were in notification.

6. Spend time setting up the call center function correctly. The huge preponderance of calls came in the first couple of days. We had staffed according to what we had heard from others' experiences, but even our very generous estimates were overwhelmed on the first day when we received a full third of all calls – likely due to email notices and media outreach.

However, outsourcing the call center function provided invaluable help in the form of daily reports and an ability to scale that allowed us to continually refine our responses and procedures very quickly. Finally, defining a procedure for escalation of angry callers was indispensable. We were lucky to have had an individual with a sympathetic ear, accurate knowledge, access to follow-up action and the stamina to handle these escalated – and usually emotionally difficult – calls.

A Privacy-Centered Approach

UCLA and the University of California respect individual privacy as a fundamental cultural and institutional value and have embedded strong protections for it in its policies. Though we have no desire to be in a situation where we must notify individuals that their privacy has potentially been breached, once it is clear there is such a situation, we will err on the side of notifying individuals of the affected community to help protect their privacy. In essence, notification is consistent with our view of respecting individual privacy.

Beyond empowering individuals to protect against identity theft, the 2003 California notification law accelerated and intensified our institutional efforts to protect data. A 2005 University of California report included recommendations to enhance our policies for the stewardship of data and to strengthen educational activities and technical measures to protect sensitive data required to be collected in the normal conduct of the business of the University. UCLA, along with the other UC campuses, has been actively engaged in implementing these recommendations.

We believe avoiding retention of sensitive data is the first step. Particularly since 2003, when the California law was enacted, UCLA has made tremendous effort to reduce retention of Social Security numbers for internal business practice. In light of the breach, we have

reexamined why we keep Social Security numbers and confirmed that fundamentally, we must keep them in order to provide them to external organizations such as the Internal Revenue Service and the National Student Clearinghouse. Our ability to continue reducing retention is thus relatively modest without a concomitant reduction in the external requirements for us to provide, and therefore keep, Social Security numbers – an effective partner to incident response and notification.

The scope and technical complexity of UCLA's breach has given us some insight into what actions were effective and where there are likely to be tensions over important decisions about notification. I hope that sharing these lessons will prove valuable to others.

Attachments

1. News release: UCLA Warns of Unauthorized Access to Restricted Database
(December 12, 2006)
2. Notification letter to those in the database (December 12, 2006)
3. Follow-up letter (January 10, 2007)
4. Home page of <http://identityalert.ucla.edu>
5. News release: FBI Advises Victims of UCLA Computer Intrusion to Report Fraud to the FBI's Internet Crime Complaint Center (December 15, 2006, <http://losangeles.fbi.gov/pressrel/2006/la121506.htm>)
6. Determining the Threshold for Security Breach Notification, University of California, 2003. http://www.ucop.edu/irc/itsec/security_breach_notification.pdf

Office of Media Relations, media@support.ucla.edu
(310) 825-2585

For Immediate Use
Dec. 12, 2006

UCLA Warns of Unauthorized Access to Restricted Database

UCLA is alerting approximately 800,000 people that their names and certain personal information are contained in a restricted database that was illegally and fraudulently accessed by a sophisticated computer hacker.

This database contains certain personal information about UCLA's current and some former students, faculty and staff, some student applicants and some parents of students or applicants who applied for financial aid. Approximately 3,200 of those being notified are current or former staff and faculty of the University of California, Merced, and current or former employees of the University of California Office of the President, for which UCLA does administrative processing.

In a letter being sent to affected individuals, Acting Chancellor Norman Abrams said that personal information about at least some of the individuals was obtained by the hacker but that there is no evidence that any data has been misused. The database includes names, Social Security numbers, dates of birth, home addresses and contact information. It does not include driver's license numbers or credit card or banking information.

"We take our responsibility to safeguard personal information very seriously," Abrams said. "My primary concern is to make sure this does not happen again and to provide to the people whose data is stored in the database important information on how to minimize the risk of potential identity theft and fraud."

UCLA blocked access to the Social Security numbers and the database when suspicious activity was detected on Nov. 21 and immediately activated its information technology security incident team. UCLA also notified the FBI, which is conducting an investigation.

Even though UCLA's ongoing investigation at this time indicates only that the hacker sought and obtained some of the Social Security numbers, out of an abundance of caution, the university decided to notify all 800,000 people whose names are listed in the restricted database.

"Ensuring data security is one of the most important responsibilities we have to the campus community, and in recent years we have significantly strengthened our information security practices in response to increasing attacks. In spite of our diligence, a sophisticated

2-2-2 Database Breach

hacker found and exploited a subtle vulnerability in one of hundreds of applications,” said Jim Davis, UCLA’s chief information officer and associate vice chancellor–Information Technology. “We deeply regret the concern and inconvenience caused by this illegal activity. We have reconstructed and protected the compromised database and launched a comprehensive review of all computer security measures to accelerate systematic enhancements that were already in progress.”

UCLA began sending notification letters and e-mails on Dec. 12, as soon as possible after determining that personal data was potentially accessed and after retrieving individual contact information. The letters suggest that recipients contact credit reporting agencies and take steps to minimize the risk of potential identity theft.

To provide information and respond to queries, UCLA has established a Web site, <http://www.identityalert.ucla.edu>, and a toll-free call center, (877) 533-8082.

Davis said access to the restricted database was gained by a computer trespasser utilizing a software program designed to exploit an undetected software flaw, thereby bypassing all security measures. A problem was detected Nov. 21 when computer security technicians noticed an exceptionally high volume of suspicious database queries. An emergency investigation indicated that access attempts had been made since October 2005 and that the hacker specifically sought Social Security numbers, Davis said.

For the past decade, UCLA has been systematically upgrading computer security but had not yet identified the vulnerability maliciously exploited by the computer hacker. During this time, UCLA installed and strengthened firewalls and intrusion-detection systems, removed Social Security numbers from computer screens and written reports, and prohibited their storage on portable devices, among other steps.

The UCLA incident is the latest in a string of computer security breaches affecting financial institutions, universities and other large employers. State law requires notification when personal data is reasonably believed to have been acquired.



OFFICE OF THE CHANCELLOR
BOX 951405
LOS ANGELES, CALIFORNIA 90095-1405

December 12, 2006

Dear Friend,

UCLA computer administrators have discovered that a restricted campus database containing certain personal information has been illegally accessed by a sophisticated computer hacker. This database contains certain personal information about **UCLA's** current and some former students, faculty and staff, some student applicants and some parents of students or applicants who applied for financial aid. The database also includes current and some former faculty and staff at the **University of California, Merced**, and current and some former employees of the **University of California Office of the President**, for which UCLA does administrative processing.

I regret having to inform you that your name is in the database. While we are uncertain whether your personal information was actually obtained, we know that the hacker sought and retrieved some Social Security numbers. Therefore, I want to bring this situation to your attention and urge you to take actions to minimize your potential risk of identity theft. I emphasize that we have no evidence that personal information has been misused.

The information stored on the affected database includes names and Social Security numbers, dates of birth, home addresses and contact information. It does not include driver's license numbers or credit card or banking information.

Only designated users whose jobs require working with the restricted data are given passwords to access this database. However, an unauthorized person exploited a previously undetected software flaw and fraudulently accessed the database between October 2005 and November 2006. When UCLA discovered this activity on Nov. 21, 2006, computer security staff immediately blocked all access to Social Security numbers and began an emergency investigation. While UCLA currently utilizes sophisticated information security measures to protect this database, several measures that were already under way have been accelerated.

In addition, UCLA has notified the FBI, which is conducting its own investigation. We began notifying those individuals in the affected database as soon as possible after determining that personal data was accessed and after we retrieved individual contact information.

As a precaution, I recommend that you place a fraud alert on your consumer credit file. By doing so, you let creditors know to watch for unusual or suspicious activity, such as someone attempting to open a new credit card account in your name. You may also wish to consider placing a security freeze on your accounts by writing to the credit bureaus. A security freeze means that your credit history cannot be seen by potential creditors, insurance companies or employers doing background checks unless you give consent. For details on how to take these steps, please see the attachment to this letter.

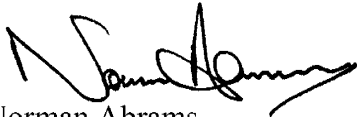
Information also is available on a Web site we have established, <http://www.identityalert.ucla.edu>. The site includes additional information on this situation, further suggestions for monitoring your credit and links to state and federal resources. If you have questions about this incident and its implications, you may call our toll-free number, (877) 533-8082.

Please be aware that dishonest people falsely identifying themselves as UCLA representatives might contact you and offer assistance. I want to assure you that UCLA will not contact you by phone, e-mail or any other method to ask you for personal information. I strongly urge you not to release any personal information in response to inquiries of this nature.

We have a responsibility to safeguard personal information, an obligation that we take very seriously.

I deeply regret any concern or inconvenience this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Norman Abrams', written in a cursive style.

Norman Abrams,
Acting Chancellor

Extensive information on steps to protect against personal identity theft and fraud are on the Web site of the California Office of Privacy Protection, a division of the state Department of Consumer Affairs, <http://www.privacy.ca.gov>.

PLACING A FRAUD ALERT

By placing a fraud alert on your consumer credit file, you let creditors know to watch for unusual or suspicious activity in any of your accounts, such as someone trying to open a credit card account in your name.

To place a fraud alert, call one of the following three major credit reporting agencies. Your phone call will take you to an automated phone system. Be sure to listen carefully to the selections and indicate that you are at risk for credit fraud.

You need only contact one of these agencies, which will automatically forward the fraud alert to the other two.

Equifax

(888) 766-0008
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
<http://www.equifax.com>

Experian

(888) 397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
<http://www.experian.com>

TransUnion

(800) 680-7289
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
<http://www.tuc.com>

Soon after you place a fraud alert, you will receive credit reports by mail from all three credit reporting agencies. In the credit report:

- Check your personal information, including home address, Social Security number, etc., for accuracy.
- Look for any charges you didn't make.
- Watch for any accounts you didn't open.
- Note any inquiries from creditors that you didn't initiate.

If you find anything that looks wrong or suspicious or that you don't understand, call the credit agency at the telephone number listed on your credit report. You may also wish to call your local police or sheriff's office to file a report of identity theft.

PLACING A SECURITY FREEZE

A security freeze means that your credit file cannot be shared with potential creditors. If your credit files are frozen, even someone who has your name and Social Security number would probably not be able to get credit in your name. A security freeze is free to those who have a police report of identity theft. If you don't have a police report, it costs \$10 to place a freeze with each credit bureau, for a total of \$30. The credit bureaus require that freeze requests be made in writing.

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

- Send by certified mail.
- Include name, current and former address, Social Security number and date of birth.
- Pay by check, money order or credit card (Visa, Master Card, American Express or Discover only). Give name of credit card, account number and expiration date.

Experian Security Freeze

P. O. Box 9554

Allen, TX 75013

- Send by certified mail.
- Include full name, with middle initial and Jr./Sr., etc.
- Include current address and home addresses for past five years, Social Security number, birth date and two proofs of residence (copy of driver's license, utility bill, insurance statement, bank statement).
- Pay by check, money order or credit card. Give name of credit card, account number and expiration date.

TransUnion Security Freeze

P. O. Box 6790

Fullerton, CA 92834

- Send by regular or certified mail.
- Include first name, middle initial, last name, Jr., etc.
- Current home address and addresses for past five years, Social Security number and birth date.
- Pay by check, money order or credit card. Give name of credit card, account number and expiration date.



OFFICE OF THE CHANCELLOR
BOX 951405
LOS ANGELES, CALIFORNIA 90095-1405

January 10, 2007

Dear:

I am writing to provide you with additional information regarding the database security incident announced in December. At that time, UCLA announced that a sophisticated computer hacker illegally accessed a database containing certain personal information and that the hacker sought and obtained at least some Social Security numbers. Through our continuing investigation, we have now confirmed that the hacker retrieved approximately 28,600 Social Security numbers. These Social Security numbers related to approximately 18,500 UCLA student financial aid applicants from 2002 through 2006 and approximately 10,100 former employees who separated from UCLA, the University of California Office of the President and UC Merced between 1995 and 2003, plus one who left in 1988.

We wanted to immediately notify members of these groups that their data was accessed by the hacker. I am very sorry to report that your Social Security number was among the 28,600 illegally retrieved. This does not mean that you are the victim of identity theft or that we have evidence of your Social Security number being misused. And it is important to know that the database does not include banking or credit card information or driver's license numbers. However, I want to reiterate my previous recommendation that you take steps to protect against potential fraud.

The attachment to this letter provides information on how to place a fraud alert on your consumer credit file. By doing so, you let creditors know to watch for unusual or suspicious activity, such as someone attempting to open a new credit card account in your name. A fraud alert, which can be reinstated after the initial 90-day period, also entitles you to a free credit report from each of the three national credit bureaus. In addition to free credit reports available to those placing fraud alerts, federal law entitles consumers to one free credit report from each credit bureau once a year. By staggering the times at which free credit reports are ordered, consumers can monitor their own credit.

There are many resources available at the special Web site we have established, <http://www.identityalert.ucla.edu>, including links to useful sites operated by the U.S. Department of Justice, the Federal Trade Commission, the California Office of Privacy Protection, and the Identity Theft Resource Center. If you have questions about this incident and its implications, you may call our toll-free number, (877) 533-8082.

Once again, I want to express my deep regret for any concern or inconvenience this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Norman Abrams".

Norman Abrams
Acting Chancellor

Attachment



Identity Alert

[Identity Alert Home Page](#)

[Protecting Your Credit](#)

[Additional Credit Protection Options](#)

[Frequently Asked Questions](#)

[Resources](#)

[Notification Letter](#) (Dec. 12, 2006)
(text only version)

[Follow-up Letter](#) (Jan. 10, 2007)
(text only version)

[News Release](#)

This Web site has been established to provide information about an incident in which a sophisticated computer hacker illegally accessed a UCLA database. The announcement was made Dec. 12, 2006, and UCLA began notifying approximately 800,000 people whose names and certain personal information are in the database (see [Notification Letter](#)). UCLA takes seriously its responsibility to safeguard personal information and regrets the inconvenience caused by this illegal and fraudulent activity.

Key Updates:

- An ongoing investigation has found that the Social Security numbers of approximately 28,600 people in the database were illegally retrieved by the hacker. UCLA began notifying them on Jan. 10, 2007 (see [Follow-up Letter](#)). The affected parties are limited to approximately 18,500 UCLA student financial aid applicants from 2002 through 2006 and 10,100 former employees who separated from UCLA, the University of California Office of the President and UC Merced between 1995 and 2003, plus one who left in 1988. If you are in this group, it does not mean you are the victim of identity theft or that your Social Security number has been misused.
- If you want to know whether you are among the approximately 800,000 people in the database or among the 28,600 whose Social Security numbers were illegally retrieved by the hacker, call the Identity Alert Hotline established by UCLA. The phone number is (877) 533-8082. Operators may need to ask you for additional information, such as the month and day of your birth or the last four digits of your Social Security number, in order to distinguish you from others with the same name.
- Regardless of whether or not the hacker has your personal information, UCLA recommends that all those in the compromised database contact the three national credit bureaus to place a fraud alert on their credit files. This instructs creditors to watch for unusual or suspicious activity, such as someone attempting to open a new credit card account in your name. A fraud alert, which can be reinstated after the initial 90-day period, entitles consumers to a free credit report from each of the three national credit bureaus. In addition to free credit reports available to those placing fraud alerts, federal law entitles consumers to one free credit report from each credit bureau once a year. By staggering the times at which free credit reports are ordered, consumers can monitor their own credit without incurring financial costs. Details on protecting your credit are available on this site at [Protecting Your Credit](#) and [Additional Credit Protection Options](#).
- If you believe you are a victim of fraud or identity theft resulting from this hacking incident, UCLA and the FBI urge you to contact the FBI's Internet Crime Complaint Center and submit an online report. In a news

release, the FBI said: "All reports submitted will be analyzed and follow-up action taken where appropriate."

Reports can be filed at: <http://www.ic3.gov>.

The news release is at:

<http://losangeles.fbi.gov/pressrel/2006/la121506.htm>.



If you do not have Adobe Reader installed, you can down a free copy by clicking the red button to the left.

[UCLA home](#) ■ [Identity Alert Hotline: \(877\) 533-8082](#) ■ [Updated: January 9, 2007](#)



Federal Bureau of Investigation Los Angeles Division

FBI * 11000 Wilshire Blvd. * Los Angeles, Ca 90024 * 310-996-3804,3343,4402 * Fax:
310-996-3345

For Immediate Release

DATE: December 15, 2006

FBI Advises Victims of UCLA Computer Intrusion to Report Fraud to the FBI's Internet Crime Complaint Center

On December 12, 2006, UCLA alerted approximately 800,000 individuals that their names and certain personal information contained in a restricted database had been illegally accessed by a sophisticated computer hacker. This database contained certain personal information, including Social Security numbers, dates of birth and home addresses, regarding current and some former UCLA students, faculty and staff, some student applicants and some parents of students or applicants who had applied for financial aid.

The FBI has initiated an investigation into the illegal access of the computer network at UCLA to determine those responsible, the extent of the computer intrusion and potential related criminal activity.

The FBI is urging anyone who was notified by UCLA that their information has been compromised and who believe they may have been victimized further by identity theft or by other fraudulent means to contact the FBI's Internet Crime Complaint Center and submit an online report. Individuals submitting reports should clearly indicate the nature of their affiliation with UCLA including their department, major, position, the month and year of their initial affiliation with UCLA and, if applicable, the date that affiliation ended. The reports should also include information as to whether or not the complainant has had his/her identity stolen or has been the victim of other identity-related fraud since June 2005. All reports submitted will be analyzed and follow-up action taken where appropriate.

The above reports should be submitted to the FBI's Internet Crime Complaint Center at: www.ic3.gov.

UCLA will also place a link to the FBI's Internet Crime Complaint Center at www.ic3.gov on the website they have set up in connection with this matter.

Determining the Threshold for Security Breach Notification

November 25, 2003

Background

California law requires notification to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a security breach. No criteria for reasonable belief are provided in the statute. The University of California Business and Finance Bulletin IS-3 Electronic Information Resources Section IV.D identifies requirements for University of California compliance with this statute. Section IV.A, which addresses data sensitivity, requires that campuses implement procedures to provide physical and logical security of this information.

Deciding Whether or Not to Notify

Campuses should consider the factors listed below in making a determination to notify for any security incidents subject to this regulation.

The Office of Privacy Protection in the California Department of Consumer Affairs <http://www.privacy.ca.gov/recommendations/recomend.htm> recommends that the following factors be considered when making a determination to notify:

Acquisition

In determining whether unencrypted notice-triggering information has been *acquired*, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information is *in the physical possession and control* of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been *downloaded* or copied, for example: an ftp log that contains the name of a file containing notice triggering information.
3. Indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(See: <http://www.privacy.ca.gov/recommendations/secbreach.pdf>)

The University of California recommends consideration of these additional factors:

- Duration of exposure.
- Indications that *any* download or copy activity has occurred, even if there is no specific evidence that there was a download or copy of data subject to the law.
- The extent to which the compromise indicates a directed attack, such as a pattern showing the machine itself was specifically targeted.
- Indication that the attack intended to seek and collect personal information.

Campuses may use additional criteria to determine whether to notify.

Campuses should feel free to contact campus counsel at any step of the process if they have questions or want legal consultation.

Other Considerations

In addition to the factors listed above, there may be other circumstances to be considered when deciding whether or not to abide strictly by the requirements imposed by the law. As an example, although the law doesn't apply to data that is encrypted, if encrypted information is reasonably believed to have been acquired as a result of a security breach, the extent to which the encryption method would prevent the information from being used should be considered when deciding whether or not to notify.

The law states: "Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure." However, notification would be required if an employee misuses authorized access to disclose personal information. Note as well that an employee disclosing previously encrypted personal information on an unauthorized basis would trigger notification.

If there is difficulty reaching a decision whether or not there is a reasonable belief that data may have been acquired as defined by this law, campuses may also consider the potential damage to individuals if the wrong decision is made. For example, one should weigh the potential for identity theft or financial abuse if it turns out that the data had been acquired and no notice was sent.