Appendix D:
Sample Notification Text

Universitywide requirements for notification of individuals when their personal identity information (PII) has been acquired by an unauthorized individual through a security breach are found in Business and Finance Bulletin, IS-3, Section III.D, Incident Response Planning and Notification Procedures.

The following text is intended to provide guidance in developing a notice to subjects of a database compromise. Sample language is also available on UCOP's Security Breach Notification website, http://www.ucop.edu/irc/itsec/securitybreach.html. The final text that is used in any actual breach notification should be reviewed by Campus Counsel.

To Whom It May Concern:

This message is being sent to you as a formal notice that personal information relating to you, and maintained in a University of California electronic information system, may have been compromised by a recent security breach. This notification constitutes the notification required pursuant to California Civil Code Section 1798.29.

The personal information which may have been obtained by an unauthorized person was contained in [*name/function of database*] and consisted of the following items of personal information: [*list data elements*].

The possible security breach consisted of [*non-technical description of scope and nature of breach, likelihood of information having been copied, etc.*].

Possible use of this information by the unauthorized person(s) might result in financial loss to you. If this is of concern, please seek advice from your bank or financial advisor. In addition, information at the following web sites might prove helpful:

- http://caag.state.ca.us/idtheft/tips.htm
- http://www.dmv.ca.gov/consumer/fraud.htm

The University has taken immediate steps to prevent a recurrence of this possible breach of security, and is investigating the possible breach for purposes of pursuing action against the individual(s) responsible, as well as finding out additional information regarding the extent to which personal information in the database was actually compromised. If you have any questions about this matter, please contact: [*insert appropriate contact person*]