APPENDIX J: Sample Breach Notice: User Name or E-Mail Address
[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*] involving the Online Information Sharing Portal (OISP). Our security systems detected an abnormally large number of attempts to access OISP user accounts. The computer generated password guessing activity was designed to randomly guess user password combinations until account access is ultimately achieved. Further investigation revealed that some user account passwords were successfully guessed before the activity was detected and blocked.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*]. Please note, the information was limited to your user identification (email address), password and security questions for your OISP online account. This incident did not involve the compromise or access to any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. However, if you use the same user identification, password and or security question for any other online accounts those may be at risk.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we have implemented additional security controls to minimize the risk associated with this occurrence and the risk of recurrence. These include prompting all system users to update their profile and reset their passwords and security questions, and implementing automated validation at password creation to ensure the use of unique, hard-to-guess passwords, and established limits on the number of failed attempts to access your account.
What You Can Do:	To protect against unauthorized access and use of your online account(s), we recommend, if you haven't already done so, that you immediately change your password and security questions. Choose a unique, hard-to-guess password for each of your online accounts and always look for and report unusual activity in your accounts. A hard-to-guess password contains at least eight characters and is a combination of upper and lower case letters, numbers and special characters.
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General".
For More Information:	For more information about online protections, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy.
AgencyContact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

_____
[*Signature of State Entity Head or Delegate*] [*Title*]