E. APPENDIX E: Sample Breach Notice - Medical Information Only*

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so. Refer to the following language.*]

Please note, the information was limited to [*specify, (e.g., your name and medical treatment)*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your medical information [*or medical history, medical condition, or medical treatment or diagnosis*] was involved.

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies for free each year by calling 1-877-322-8228 or going to the Annual Credit Report website at www.annualcreditreport.com

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For information about your medical privacy rights, we recommend you visit the website of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. 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*].

[*Closing*]

* Additional language will be necessary if other notice triggering information was involved.

F. APPENDIX F: Sample Breach Notice - Health Insurance Information Only*

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so. Refer to the following language.*]

Please note, the information was limited to [*specify, (e.g., your name and medical treatment)*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your health insurance information [*or policy, plan number, or subscriber identification number*] was involved.

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies for free each year by calling 1-877-322-8228 or going to the Annual Credit Report website at www.annualcreditreport.com

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For information about your medical privacy rights, we recommend you visit the website of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. 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*].

[*Closing*]

* Additional language will be necessary if other notice triggering information was involved.

G. APPENDIX G: Sample Breach Notice – Hybrid (SSN and Health Information)

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response*.]

Because your Social Security number was involved, and in order to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in step four of the enclosure.

Since your health insurance information [*or policy, plan number, or subscriber identification number*] was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For more information about privacy protection steps and your medical privacy rights, we recommend you visit the website of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. 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*].

[*Closing*]

Enclosure [*Enclose the Security Breach - First Steps Enclosure*]

H. APPENDIX H: Security Breach - First Steps Enclosure (English)

This document is available on the OISPP Web site at
http://www.oispp.ca.gov/consumer_privacy/pdf/Security_Breach_First_Steps.pdf

CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

www.privacy.ca.gov

Privacy Protection Recommendations

What to Do If Your Personal Information Is Compromised

1 Contact the three credit bureaus.

You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a copy of your report from each of the credit bureaus. As a possible victim of identity theft, you will not be charged for these copies.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 What it means to put a fraud alert on your credit file.

A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed.

3 Review your credit reports. Look through each one carefully.

Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4 If you find items you don't understand on your report, call the credit bureau at the number on the report.

Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved and report the crime to your local police or sheriff's office. For more information on what to do in this case, visit the California Office of Privacy Protection's Web site at www.privacy.ca.gov, and go to the Identity Theft page.

CALIFORNIA OFFICE OF INFORMATION SECURITY & PRIVACY PROTECTION
www.oispp.ca.gov

I. APPENDIX I: Security Breach - First Steps Enclosure (Spanish)

This document is available on the OISPP Web site at
http://www.oispp.ca.gov/consumer_privacy/pdf/Security_Breach_First_Steps_SP.pdf

CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

www.privacy.ca.gov

Cómo proteger su privacidad

Qué hacer si su información personal está comprometida

1 Póngase en contacto con las tres agencias de crédito.

Para informar el robo potencial de su identidad llame sin cargo a cualquiera de las tres agencias principales de crédito indicados a continuación. Accederá a un sistema telefónico automatizado para informar fraude el cual le permitirá marcar su archivo de crédito en las tres agencias de crédito con un alerta de fraude. También le enviarán instrucciones para solicitar una copia de su informe de cada una de las agencias de crédito. No tendrá que pagar por las copias del informe ya que se trata de un posible robo de identidad.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 Qué quiere decir poner un alerta de fraude en su archivo de crédito.

Un alerta de ayudará a protegerlo contra la posibilidad de que un ladrón de identidad abra cuentas nuevas de crédito en su nombre. Cuando un comerciante verifica el historial de crédito de una persona que está solicitando crédito, recibirá un aviso indicando que puede haber fraude en la cuenta. Esto alerta al comerciante a que tome pasos para verificar la identidad del solicitante. El alerta de fraude dura 90 días y se puede renovar.

3 Examine sus informes de crédito. Revise cuidadosamente cada uno de ellos.

Fíjese si hay cuentas que no reconoce, sobre todo cuentas abiertas recientemente. Fíjese en la sección de consultas para ver si hay empresas a las que no les solicitó crédito. Algunas empresas facturan bajo un nombre distinto que el nombre de la empresa. En esos casos, la agencia de crédito podrá aclarar de qué empresa se trata. Puede encontrar ciertas consultas identificadas como "promocionales". Estas consultas son efectuadas cuando una compañía obtuvo su nombre y dirección de una agencia de crédito y le envía una oferta de crédito. Las consultas promocionales no son un signo de fraude. (Cuando haga un alerta de fraude, lo eliminarán automáticamente de las listas de ofertas no solicitadas de este tipo). Como precaución general, fíjese también en la sección sobre información personal para ver si hay alguna dirección donde nunca ha vivido.

4 Si encuentra en su informe transacciones que no comprende, llame a la agencia de crédito al número que aparece en el informe.

El personal de la agencia de crédito analizará el informe junto con usted. Si no puede explicar la información usted tendrá que llamar a los acreedores involucrados e informar el delito en su comisaría u oficina del alguacil local. Para obtener más información sobre lo que tiene que hacer en este caso, visite el sitio Web de la Oficina de Protección de Privacidad de California en www.privacy.ca.gov y vaya a la página de Robo de identidad *(Identity Theft)*.

California Office of Information Security & Privacy Protection
www.oispp.ca.gov