CALPINE CORPORATION

717 Texas St., Ste. 1000
Houston, Texas 77002
(713) 830-2000

[Return Address]
[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Notice of Data Breach
Important Security and Protection Notification
Please read this entire letter.

Dear [Insert employee name]:

We are writing to let you know about a potential data security incident, which occurred on February 9, 2016.

What Happened

A Calpine employee's laptop, which contained confidential employee information, was stolen from a car. We learned from law enforcement that the car that was broken into is one of several cars broken into on the same day, in the same general vicinity. We believe that the theft was likely conducted by someone interested in the value of hardware stolen as opposed to information or files on the computer. In addition, the computer was password protected and contained software that would cause the computer to be immediately wiped if the unauthorized user connected to the Internet. Also, the financial information on the laptop was maintained in a format that would make it difficult for a bad actor to exploit.

For these reasons, we believe that it is unlikely that your information will be misused and, at this time, we have no evidence to suggest that any misuse has occurred as a result of this incident. However, in order to prevent and detect misuse of your information, we strongly encourage you to take the preventative measures outlined in this letter.

What Information Was Involved

The information contained on the laptop may have included your name, Social Security Number, bank account and routing number, payroll direct deposit net pay amount, and 401k deduction amount. However, as mentioned, based on the circumstances surrounding the crime and technical controls on the computer on which the information resided, we believe it is unlikely that the information will be accessed or misused.

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. We take the protection of your information very seriously, and we apologize for what occurred here. As soon as this incident was

discovered, law enforcement was immediately notified. We are conducting a thorough review of the potentially affected records and are implementing additional security measures, internal controls, and safeguards and are making changes to existing policies and procedures designed to prevent a similar occurrence from happening again. Please notify us at your earliest convenience by sending an email to datasecurityquestions@calpine.com, if you become aware of any misuse of your personal information.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

What You Can Do

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: [date]** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/alert**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide engagement #: **[engagement number].**

Additional details regarding your 12-MONTH ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian credit report.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-297-7780.

For More Information

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). We have also provided resources where you can obtain additional information about identity theft and ways to protect yourself. Please refer to the final page of this letter for this information.

We sincerely apologize for this incident, regret any inconvenience it may cause you, and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to call (877) 297-7780.

Sincerely,

Hether Benjamin Brown
Sr. Vice President and Chief Administrative Officer

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG . The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or 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. 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, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.