Davis Wright Tremaine LLP

Suite 800
1919 Pennsylvania Avenue N.W.
Washington, D.C. 20006-3401

Christin McMeley
202-973-4264 tel
202-973-4464 fax

christinmcmeley@dwt.com

April 18, 2016

Office of the New Hampshire Attorney General
Attorney General
33 Capitol Street
Concord, NH 03301

Re: Report of Data Breach

To the Office of the New Hampshire Attorney General:

I represent DealerSocket Inc. (DealerSocket). The business is located at 100 Avenida La Pata, San Clemente, CA 92673. Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, I am writing to notify you of an unauthorized disclosure of personal information involving two (2) residents of New Hampshire.

On April 11, 2016, DealerSocket was the target of a phishing email scheme that purported to be from a DealerSocket executive leader and requested personal information about employees. The information involved included the personal information found in employees' W-2, including their: (i) full name; (ii) home address; (iii) social security number; and (iv) 2015 earnings as a DealerSocket employee. The information involved did not include (i) any other information that may have been available or provided during the DealerSocket onboarding process; (ii) employee background check screening; (iii) health information; or (iv) other demographic information.

DealerSocket is in the process of implementing additional security measures and user education designed to prevent a recurrence of a fraudulent phishing scheme. DealerSocket is also working with the United States Internal Revenue Service, Criminal Investigation Unit, to help identify the taxpayer information at risk so that the agency can take appropriate measures to identify attempted fraudulent tax filings. As an added precaution, DealerSocket has arranged to have AllClear ID provide credit monitoring and identity repair services for three years at no cost to the affected individuals.

Should a perpetrator be identified and convicted, DealerSocket requests the opportunity to submit a victim impact statement and a request for restitution for all costs related to the breach.

Please contact me should you have any questions.

Sincerely,

Christin McMeley, CIPP/US

Enclosure: Representative sample notification letter to New Hampshire residents.

DealerSocket®

100 Avenida La Pata, San Clemente, CA 92673

April 18, 2016

[Employee/Former Employee Name]
[Address Line 1]
[Address Line 2]

Notice of Data Breach

We are writing to you about a data security incident involving your personal information that occurred on April 11, 2016. This letter supplements information you may have previously received and more fully describes what happened and what you should do now.

What Happened? On April 11, 2016, DealerSocket was the target of a phishing email scheme that purported to be from a DealerSocket executive leader and requested personal information about employees.

What Information Was Involved? The information involved included the personal information found in your W-2, including your: (i) full name; (ii) home address; (iii) social security number; and (iv) 2015 earnings as a DealerSocket employee. The information involved did not include (i) any other information that may have been available or provided during your DealerSocket onboarding process; (ii) employee background check screening; (iii) health information; or (iv) other demographic information.

What We Are Doing. We are in process of implementing additional security measures and user education designed to prevent a recurrence of a fraudulent phishing scheme. We are also working with the United States Internal Revenue Service, Criminal Investigation Unit, to help them identify the taxpayer information at risk so that the agency can take appropriate measures to identify attempted fraudulent tax filings.

As an added precaution, we have arranged to have AllClear ID protect your identity for 36 months, at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months:

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required so long as you enroll in AllClear Pro. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at https://enroll.allclearid.com using the following redemption code: {RedemptionCode}.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What You Can Do. In addition to enrolling in the service described above, if you believe you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify any questionable activity, please complete Form 14039, Identify Theft Affidavit, available at https://www.irs.gov/pub/irs-pdf/f14039.pdf, and submit it to the appropriate address per the form instructions. You also may contact the IRS's Identity Protection Specialized Unit (IPSU) at 800-908-4490. For additional information Identity Theft Prevention and Victim Assistance, you can review IRS Publication 4535, available at https://www.irs.gov/pub/irs-pdf/p4535.pdf.

Other Important Information. Please review the "Further Steps and Contact List" information on the reverse side of this letter which identifies additional steps to take to protect your information.

For More Information. Please contact us at: employeequestions@dealersocket.com.

We take all security incidents seriously, and we will continue to provide updates as appropriate.

Sincerely,

R. Cameron Darby
COO & General Counsel

FURTHER STEPS AND CONTACT LIST
STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 9554
Allen, TX 750133

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834

Fraud Alert

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft

You can obtain information from the consumer reporting agencies, FTC or from your respective state Attorney General about steps you can take toward preventing identity theft including placing fraud alerts and security freezes. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of *Taking Charge: What to Do if Your Identity is Stolen*, an FTC guide to help you guard against and deal with identity theft, can be found at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

MD Attorney General
200 St. Paul Place
Baltimore, MC 21202
oag.state.md.us
1-888-743-0023

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226