LAW OFFICES OF
DAVID A. KRAUSZ, P.C.

2740 VAN NESS AVENUE, SUITE 300
SAN FRANCISCO, CA 94109-1463
TELEPHONE: (415) 567-5000
WWW.LODAKPC.COM

January 12, 2015

Dear Client:

On January 6, 2015, Law Offices of David A. Krausz, P.C. experienced the theft of a laptop computer that contained identifying client information including names, social security numbers and dates of birth. As a result of this incident, information identifiable with you was ***potentially*** exposed to others. The theft was reported to the San Francisco Police Department and a report was filed.

Out of an abundance of caution, however, Law Offices of David A. Krausz, P.C. is taking all possible steps to protect and inform our clients. While you do not need to take any action unless you are aware of suspicious activity regarding your personal information, there are steps you may take to protect against identify theft and we wanted you to be aware of these. The Federal Trade Commission website suggests taking the following steps if your personal information has been compromised. Call the toll-free fraud number of any *one* of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. A fraud alert lets creditors know to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus using the information listed below. The company you contact is required to notify the other two, which will place an alert on their versions of your credit report as well. An initial fraud alert stays on your credit report for 90 days.

Equifax: (800) 525-6285; www.equifax.com; P.O. Box 740231, Atlanta, GA 30374-0241

Experian: (888) 397-3742; www.experian.com; P.O. Box 2002, Allen, TX 75013;

TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

When you place the alert, you will get information about ordering one free credit report from each of the companies. It is prudent to wait about a month after your information was stolen before you order your report. That is because suspicious activity may not show up right away. Once you get your reports, review them for suspicious activity, like inquiries from companies you did not contact, accounts you did not open, and debts on your account that you cannot explain. Check that the information - such as your social security number, address, name and employers is correct. In addition, please be aware of any phone calls, e-mails or other communications from individuals asking for your personal information or verification of it. This is often referred to as information solicitation or "phishing" Legitimate organizations will not contact you to ask for or confirm your personal information.

We regret this incident and inconvenience or concern this situation may cause, but we believe it is important for you to be fully informed of any potential risk resulting from this incident. Again we want to reassure you we have no evidence that your protected data has been misused. We take our obligation to serve our current and former clients very seriously and we are committed to protecting your privacy at the highest level possible.

Sincerely,

David A. Krausz