ZIPRICK & CRAMER, LLP
ATTORNEYS AT LAW

707 BROOKSIDE AVENUE
REDLANDS, CA 92373-5101
PHONE: (909) 798-5005

February 27, 2015

Dear Clients,

It is almost a daily occurrence that we read about cyberattacks in the news: the Department of Defense, Sony Pictures, Anthem Blue Cross, Facebook, Gmail and many others. Until now, we at Ziprick & Cramer, LLP, have never had any virus or malware get through our various layers of computer protections. Unfortunately, on or around January 25, 2015, our firm was the victim of a single cyberattack, by a relatively new variant of a Cryptolocker-type virus (which is a fairly sophisticated form of ransomware, which is apparently being used by criminals around the world). It infected one of our workstations (with the virus encrypting data on the workstation), and then traveled to the in-house server where data was also encrypted on shared folders (collectively, the "Computer"). Accordingly, we are sending this notification letter to all clients for whom we had any data on the Computer.

After the cyberattack, we immediately brought in our computer specialist who has worked extensively with us over these last few weeks to assess the attack, to determine what information was encrypted, and what additional safeguards can be implemented to provide further defense against cyberattacks in the future. The infected work station was removed, which was where the virus program was located. Our specialist contacted our antivirus and malware protection companies' experts, providing them details of the cyberattack and consulted with them in fighting the Cryptolocker-type virus. In summary, our information is that this virus is being used in attacks globally, and that the consistent pattern of this virus is to encrypt files. The hackers then demand a ransom and threaten to destroy the data if the ransom is not paid. Our firm did not and will not pay any such ransom, which would only encourage and fund such criminals in their illegal activities.

We are advised that the usual pattern for this ransomware virus does not include downloading of data. While we have discovered no evidence that any downloading of data occurred here, our goal, if possible, is to get a conclusive opinion from a computer forensics expert whether data was copied or whether it was simply encrypted.

Because of backups, the parts of our computer system which were not impacted and hard copies of documents and correspondence, etc., we believe the loss of data is fairly minimal. During these past weeks, we, with our computer specialist and software protection experts have been working to assess, recover, and work to prevent such cyberattacks in the future.

We have reported this cyberattack to the FBI, and have promised our full cooperation with them. Further, our firm is implementing even more layers of protection and safeguards for our computer system, as we want to best prevent such criminal hackers for any future successful attacks.

Although we have no evidence that any information was downloaded, we want to also assure you that any illegal access to information in our computer system does not waive the attorney/client privilege. That privilege can only be waived by the client.

For notification purposes, the State of California has defined "personal information" as the following:

- Social Security Number
- Driver's License or Identification Card Number
- Account Number, Credit or Debit Card Number, but only in combination with any required code or password permitting access to an individual's financial account
- Medical Information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.
- Health Insurance Information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individuals' application or claims history, including any appeals records.

For the majority of our clients, we did not have any such personal information on the Computer, and accordingly, for such clients no personal information was impacted by this cyberattack. We have been in the process of reviewing through the data which was on the Computer to identify clients for which personal information was impacted. **However, in the interests of time, and as a precautionary safeguard to all of our clients who are individuals (including the individual owners of our clients which are entities), we are offering you the option to enroll, <u>at no cost to you</u>, in an online credit monitoring service, My TransUnion Monitoring, for one (1) year. That service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies. To enroll free of charge for the service, please follow the instructions described on the last page of this letter.**

While we have no evidence that data on the Computer was downloaded, we want to provide you with the following resource information concerning steps that you can take to safeguard against any possible identity theft.

Social Security Number: Because your Social Security number may have been involved, to be conservative, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify

your identity before issuing credit in your name. A fraud alert lasts for 90 days. To do this, call one of the three credit reporting agencies at a number below. This will let you automatically place an alert with all of the agencies. You should receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

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

Each credit bureau also has fraud alert information on the internet:

Experian: http://www.experian.com/fraud

TransUnion: http://www.transunion.com/fraud

Equifax: https://www.alerts.equifax.com

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or Sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. You can keep the fraud alert in place by calling again after 90 days.

California Driver's License or Identification Card Number: We do not routinely have our clients' driver's license or identification card numbers. However, there are certain situations, such as in litigation matters, where the standard form of Interrogatories asks for the driver's license number of the responding party. Accordingly, if you believe you provided your driver's license number to our firm, you may call the DMV Fraud Hotline at 1-866-658-5758 to report it. The Hotline will allow you to put a 30 day "Courtesy Control" on your driver's license, which blocks it from access through systems (banks and law enforcement will not be able to verify your license through their automated systems). At the end of 30 days, DMV will send you a letter asking you if you would like to extend the Courtesy Control for another year. At the end of 13 months, the Courtesy Control will automatically drop off your license, or if you want it removed earlier, you can fax a letter to DMV with the request.

Financial Account Numbers: We do not believe that we had for any of our clients Financial Account Numbers, in combination with any required code or password permitting access to an individual's financial account on the Computer. Further, we do not keep client credit card information on the Computer.

Medical Information or Health Insurance Information: Our firm rarely, if ever, has any health insurance related information on clients. As to medical information, we have a relatively small number of clients which have provided medical information to us.

However, as a general practice we recommend that you regularly review the explanation of benefits statement that you receive from your health insurer. If you see any service that you believe you did not receive, please contact your health insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

Check for any medical bills on your credit reports that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report.

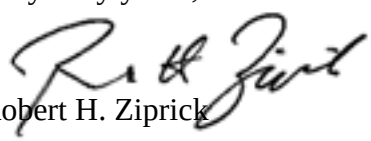
Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider or plan to serve as a baseline.

We also want to provide you with contact information for the website of the California Office of Privacy Protection (www.privacy.ca.gov) for additional information for California residents for protection against identity theft.

In the event you have any questions regarding this incident, please contact us at our toll-free number (877-931-1373) or our regular office number (909-798-5005).

We greatly appreciate each and every one of you, and are sorry for any inconvenience this has caused. We want to assure you that we take our commitment to diligently represent and protect our clients' interests seriously.

Very truly yours,



Robert H. Ziprick

William F. Ziprick

Enc. How to Sign Up for the Free Credit Monitoring Services,
with personalized Activation Code

ZIPRICK & CRAMER, LLP
ATTORNEYS AT LAW

707 BROOKSIDE AVENUE
REDLANDS, CA 92373-5101
PHONE: (909) 798-5005

How to Sign Up for the Free Credit Monitoring Services

Complimentary Three-Bureau Credit Monitoring Service
As a safeguard, we are offering you the option to enroll, at no cost to you, in an online credit monitoring service (*My TransUnion Monitoring*) for one (1) year which service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies.

To enroll via the internet to this free service, go to the TransUnion Monitoring website at **www.transunionmonitoring.com** and in the space referenced as "Activation Code", enter the following unique 12-letter Activation Code:

XXXXXXXXXXXX

Then follow the simple steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet, please contact our firm and we can arrange for you to come to our office and sign up over the internet.

You can sign up for the online credit monitoring service anytime between now and **June 30, 2015**.

Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Additional Free Credit Report Information
Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies (separate from the Transunion service you may sign up for). Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Security Freeze Information
You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report.

This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Please contact each of following credit bureaus to place a Security Freeze on your credit files at each credit bureau:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

TransUnion Security Freeze
PO Box 2000
Chester, PA 19022
http://transunion.com/securityfreeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742