LAW OFFICES OF
BOBBY P. LUNA

March 28, 2024

VIA EMAIL

Re: *Notice of Potential Data Breach*

Dear Clients:

The Law Offices of Bobby P. Luna recently experienced a data security incident that may have affected your personal information. Based on our understanding of the issue, we have no indication that your personal information has been, can be, or will even be accessed. However, out of an abundance of caution, we wanted to make you aware of the incident and the measures we have taken in response. We also wanted to provide details on the steps you can take, should you deem it appropriate, to help protect your information. **Again, let us be clear that our IT professionals do not have any confirmation that any of your information has been accessed**. The protection and proper use of your information is a top priority for the Law Offices of Bobby P. Luna, and we are working to prevent a similar incident from occurring again in the future. In an abundance of caution, we are providing you information about the incident, our response, and steps you can take to protect your information should you feel it is necessary to do so.

What Happened?

On March 18, 2024, the Law Offices of Bobby P. Luna experienced a ***ransomware*** attack in which an unauthorized third party accessed and encrypted data from our network computer system. This was discovered on the morning of March 19, 2024, and we immediately began working with our IT provider to remedy and retrieve the data. The infected device was immediately isolated and removed from the system. At this point, our IT provider has been unsuccessful in decrypting the infected files. Unfortunately, these types of incidents are becoming increasingly common and even organizations with the most sophisticated IT infrastructure have been affected. We have worked diligently to determine what happened and continue to work to retrieve the data that was breached.

What Information Was Involved?

The information stored in this platform include any information you may have provided to us during the totality of your case. The elements of your personal information that **might** have been impacted include: Your Name/Your Spouses/Your Child's: Name, Date of Birth, Social Security number, Driver's License or Identification card number, Tax ID number, Passport number, Financial Account number, Bank statements, Credit Card statements, Medical information, Health Insurance information, Tax Returns, Employee information, Court Orders, as well as legally privileged/protected information, including legal documents, case notes, disclosures, evidence, photos, invoices, transcripts, and attorney-client communications.

BOBBY P. LUNA, C.F.L.S.*
*Certified Specialist- Family Law
State Bar of California,
Board of Legal Specialization
bobby@lunafamilylaw.com

JENNIFER B. HOLDENER, C.F.L.S.*
*Certified Specialist- Family Law
State Bar of California,
Board of Legal Specialization
jennifer@lunafamilylaw.com

SACRAMENTO
1545 River Park Drive
Suite 300
Sacramento, CA 95815
Phone: (916) 514-9349
Fax: (916) 514-9373

We do not have any information indicating that your personal information has been accessed or misused in any way. **As stated above, the infected device was immediately removed and the information contained therein is not presently accessible. Please note, that we do not store ANY payment information, such as credit card information used for payments into this system.**

What We Are Doing:

We have notified local law enforcement of this breach, as well as the Federal Bureau of Investigations. Our IT provider is currently implementing new systems to avoid this type of event in the future. We are taking this incident very seriously and are committed to strengthening our security systems to prevent a similar event from occurring in the future.

What You Can Do:

At this time, we are not aware of anyone experiencing any access or fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant. You should remain aware for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. Promptly report incidents of suspected identity theft or suspicious activity. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

Other Important Information:

Any evidence of identity theft and fraud should be immediately reported to the local authorities, the Federal Bureau of Investigation, the Federal Trade Commission, and the Department of Justice. The contact information for these agencies can be found online, or you can call us at (916) 514-9349 and we will provide you with this information.

For More Information:

As we receive additional relevant information, we will reach out to you and provide further updates. Please do not hesitate to contact this office should you have any questions or concerns.

Sincerely,

LAW OFFICES OF BOBBY P. LUNA

By:_____
Bobby P. Luna, Esq.

Additional Important Information

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are located below.

Monitoring:

You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, tollfree, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report. Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

Security Freeze:
You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well):

(1) full name, with middle initial and any suffixes;
(2) Social Security number;
(3) date of birth;
(4) current address and any previous addresses for the past five years; and
(5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax	Experian	TransUnion
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Security Freeze** P.O. Box 105788 Atlanta, GA 30348 equifax.com/personal/credit-reportservices/ 1-800-349-9960	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 experian.com/freeze/center.html 1-888-397-3742	**TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016 **TransUnion Security Freeze** P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed below.

Implementing an Identity Protection PIN (IP PIN) with the IRS:
To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identityprotection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:
• An IP PIN is valid for one calendar year.
• A new IP PIN is generated each year for your account.
• Logging back into the Get an IP PIN tool, will display your current IP PIN.
• An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

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