LEWIS BRISBOIS BISGAARD & SMITH LLP

Brian Craig
2112 Pennsylvania Avenue, NW, Suite 500
Washington DC, 20037
Brian.Craig@lewisbrisbois.com
Direct: 202.926.2904

May 14, 2021

VIA EMAIL
Attorney General Tom Miller
Office of the Attorney General
Consumer Protection Division
Security Breach Notifications
1305 E Walnut Street
Des Moines, IA 50319-0106
Email: consumer@ag.iowa.gov

Re: Notification of Data Security Incident

Dear Attorney General Miller:

We represent Phillip Galyen, PC ("Galyen"), a law firm located in Bedford Texas, in connection with a recent data security incident described below. Galyen has notified the affected individuals of the incident. The purpose of this letter is to provide formal notice to your office.

I. Nature of the Security Incident

In March 2021, Galyen discovered malicious activity within their environment. Upon learning of this activity, they took steps to secure the digital environment and began an investigation to determine what happened. In so doing, Galyen engaged independent cyber experts to determine what happened and whether personal information may have been accessed or acquired without authorization. The investigation discovered that a malicious actor may have accessed the Galyen network without authorization. The malicious actor may have also accessed and acquired certain personal information associated with of clients and employees of Galyen. The information may include individuals' names, dates of birth, driver's license or personal identification card numbers, Social Security Numbers, payment account numbers, payment card information, biometric data including but not limited to medical information and history, medical diagnosis and treatment information, health insurance information, and other personal information.

Galyen is notifying the affected residents via substitute notice, which includes a notice on the Galyen website and a press release to statewide media. All impacted persons will have access to credit monitoring services.

II. Number of Iowa Residents Affected

Over the course of the investigation, Galyen determined that some data was accessed within their environment. However, due to the nature of the environment and the forensic evidence available, Galyen was not able to determine exactly which information may have been accessed. Galyen's clients are primarily located in Texas, but they do have some clients throughout the country. As a result, Galyen is notifying all potentially affected Iowa residents via substitute notice.

III. Actions Taken in Response to the Incident

As soon as Galyen detected a potential incident, it launched an investigation, engaged a digital forensics firm, and worked to determine whether any personal information was accessed or acquired without authorization. This includes working with leading cybersecurity experts to enhance the security of their digital environment.

Galyen submitted a press release to statewide media and placed a notice of the incident on their website. Galyen is also offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and Cyberscan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 202.926.2904 or Brian.Craig@lewisbrisbois.com.

Very truly yours,

Brian Craig of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Notice of Potential Data Security Incident

May 14, 2021 - A recent potential data security incident experienced by Phillip Galyen P.C. ("Galyen") may have impacted personal information of clients and employees of Galyen. At Galyen, we take the privacy and security of individuals personal information very seriously. We are posting this notification to inform the public about steps individuals can take to protect personal information.

What Happened? In March 2021, the Galyen IT department discovered unusual activity within their network environment. Galyen conducted an investigation and hired independent computer forensic investigators to help determine what happened. The investigation discovered that a malicious actor may have accessed the Galyen network without authorization. The malicious actor may have accessed and acquired certain personal information associated with clients and employees of Galyen.

What Information Was Involved? This incident may have involved information individuals provided to Galyen in connection with their representation or employment. The information may include individuals' names, dates of birth, driver's license or personal identification card numbers, Social Security Numbers, payment account numbers, payment card information, biometric data including but not limited to medical information and history, medical diagnosis and treatment information, health insurance information, and other personal information.

What Are We Doing? As soon as the incident was discovered Galyen took the steps described above. Galyen is notifying potentially impacted individuals through this website notice. In addition, Galyen is offering certain individuals who may have been impacted with information about steps they can take to help protect their personal information, along with complimentary credit monitoring and identity remediation services. Further, Galyen reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to help prevent fraudulent activity and facilitate prosecution of the perpetrators.

For more information: If you have any questions or think your personal information may have been affected, can confirm your connection to Galyen, and would like to inquire about enrolling in the free credit and identity monitoring services, please call 833-752-0861, Monday through Friday from 8:00 AM to 8:00 PM Central Time.

Steps You Can Take to Protect Your Personal Information: While Galyen not aware of the misuse of any information involved in this incident, Galyen encourages potentially affected individuals to remain vigilant by taking the following steps:

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). Under Rhode Island and Massachusetts law, you have the right to file a police report in connection with this incident.

Federal Trade Commission	**Rhode Island**	**Maryland Attorney General**	**North Carolina Attorney General**
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400	200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226

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:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000 Chester, PA19016 1-800-909-8872 www.transunion.com	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 105851 Atlanta, GA 30348 1-800-685-1111 www.equifax.com	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com

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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission,** 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.