LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

July 17, 2020

**VIA Email: DOJ-CPB@doj.nh.gov**
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: Notification of Data Security Incident

To Attorney General MacDonald:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Verigent, LLC ("Verigent") in connection with the recent data security incident described in greater detail below. The privacy and security of all information within Verigent's possession is extremely important to Verigent. As such, in addition to providing notification of this incident to potentially impacted individuals, Verigent has taken significant steps to help prevent similar incidents from occurring in the future.

**1. Nature of the security incident.**

On January 3, 2020, Verigent learned of a suspicious email sent from a Verigent employee's email account. Upon learning of this suspicious message, Verigent took steps to secure its email system and engaged an independent digital forensics firm to conduct an investigation. As a result, Verigent learned on January 28, 2020 that certain employee email accounts had been accessed without authorization. Verigent then engaged a document review vendor to review the contents of the accounts believed to contain personal information. On June 4, 2020, as a result of this review, Verigent learned that the personal information of certain New Hampshire residents may have been accessed without authorization as a result of this incident. Verigent then worked diligently to identify up-to-date address information and to provide notification to potentially impacted individuals.

**2. Number of New Hampshire residents.**

Verigent notified 9 New Hampshire residents of this data security incident via first class U.S. mail on July 17, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

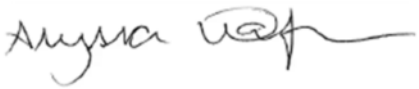
**3. Steps taken relating to the incident.**

As set forth in the enclosed letter, Verigent has taken steps in response to this incident to help prevent similar incidents from occurring in the future. Those steps have included, among other things, working with leading cybersecurity experts to enhance the security of its digital environment and implementing multi-factor authentication. Furthermore, out of an abundance of caution, Verigent is also providing complimentary credit monitoring and identity theft restoration services to each letter recipient through ID Experts, a data breach and recovery services expert.

**4. Contact information.**

Verigent remains dedicated to the protection of all personal information within its control. If you have any questions or need additional information, please do not hesitate to contact me at 720-292-2052 or Alyssa.Watzman@lewisbrisbois.com.

Sincerely,



Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

Verigent
Works for you.

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

**<<FirstName>> <<LastName>>**
**<<Address1>>**
**<<Address2>>**
**<<City>>, <<State>> <<Zip Code>>**

To Enroll, Please Call:

833-431-1277

Or Visit:
https://app.myidcare.com/account-creation/protect

Enrollment Code: <<XXXXXXXX>>

July 17, 2020

Re: Notice of Data Breach

Dear **<<FirstName>> <<LastName>>**:

We are writing to inform you of a data security incident experienced by Verigent, LLC ("Verigent") that may have affected your personal information. The privacy and security of your information is extremely important to Verigent. That is why we are writing to inform you of this incident, to offer you complimentary credit monitoring and identity theft restoration services, and to provide you with information relating to steps that can be taken to help protect your information.

**What Happened?** On January 3, 2020, Verigent learned of a suspicious email sent from a Verigent employee's email account. Upon learning of this suspicious message, Verigent immediately took steps to secure its email environment which included resetting the passwords required to access all Verigent employee email accounts and implementing multi-factor authentication. Verigent also began a preliminary investigation and engaged an independent forensics firm to assist. On January 28, 2020, the forensics firm informed Verigent that an unauthorized individual had gained access to certain Verigent employee email accounts. On June 4, 2020, Verigent learned that the email accounts accessed without authorization contained some of your personal information which may have been viewed by an unauthorized individual. Verigent then worked diligently to identify up-to-date address information in order to provide notification to potentially impacted individuals.

Please note that this incident was limited to potential unauthorized access to information transmitted via email and did not affect any other Verigent information systems. Please also note that Verigent has no evidence to suggest that your personal information has been misused in connection with this incident.

**What Information Was Involved?** The information impacted in connection with this incident may have included your name as well as your address, date of birth, Social Security number, passport number, driver's license or other government issued identification number, digital signature, financial account / payment card information, medical information, and/or online credentials.

**What Are We Doing?** As soon as Verigent discovered this incident, we took the steps described above. In addition, because we take the confidentiality of all information within our possession very seriously, we have taken steps to enhance the security of our email environment in order to minimize the likelihood of similar incidents occurring in the future. In addition, we reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators of this incident accountable.

We are also providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering you complimentary credit monitoring and identity theft restoration services through ID Experts®, a data breach and recovery services expert. MyIDCare™ services include: <<twelve (12) / twenty-four (24)>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in MyIDCare™ by calling 833-431-1277 or by going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare™ experts are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Standard Time. Please note the deadline in these services to enroll is October 17, 2020.

To receive these services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive these services by mail instead of online, please call 833-431-1277.

**What You Can Do:** You can follow the recommendations attached to this letter to help protect your personal information. We recommend that you review your credit report and consider placing a security freeze on your credit file. We also recommend that you enroll in the free MyIDCare™ services referenced herein.

**For More Information:** Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call ID Experts at 833-431-1277 from 9:00 a.m. to 9:00 p.m. Eastern Standard Time, Monday through Friday.

We take your trust in us and this matter very seriously and we apologize for any worry or inconvenience that this incident may cause you.

Sincerely,

Rebecca Hardin
Chief Financial Officer
Verigent, LLC

## 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:

| **TransUnion** | **Experian** | **Equifax** | **Free Annual Report** |
|---|---|---|---|
| P.O. Box 1000 | P.O. Box 9532 | P.O. Box 105851 | P.O. Box 105281 |
| Chester, PA 19016 | Allen, TX 75013 | Atlanta, GA 30348 | Atlanta, GA 30348 |
| 1-800-916-8800 | 1-888-397-3742 | 1-800-525-6285 | 1-877-322-8228 |
| www.transunion.com | www.experian.com | www.equifax.com | 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:** 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. There is no charge 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**: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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

**Washington D.C. Attorney General**
441 4th Street, NW
Washington, DC 20001
https://oag.dc.gov/
202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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.