Lindsey Smith
145 West Ostend Street
Suite 600
Baltimore, Maryland 21230
ldsmith@constangy.com
706.247.3613

September 26, 2025

VIA ONLINE SUBMISSION
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP, represents Business Integra Technology Solutions, Inc. ("Business Integra") in conjunction with their response to a recent security incident discussed below. Business Integra is an IT services and staffing support provider located in Bethesda, MD. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute, N.H. Rev. Stat. §§ 359-C:19-21.

1. Nature of the Security Incident

On August 23, 2025, Business Integra experienced a network disruption and immediately began investigating with the assistance of independent cybersecurity experts. As a result of the investigation, we determined that certain files were potentially acquired without authorization. Business Integra then reviewed the files, and on September 11, 2025, we learned that personal information was contained in the affected data. Please note that Business Integra has no evidence of the misuse, or attempted misuse, of the information.

2. Number of New Hampshire Residents Affected

The incident involved personal information for 1 New Hampshire resident. The information involved in the incident may differ depending on the individual but may include the following for affected New Hampshire residents: name, Social Security number, driver's license, and financial account information.

3. Notification to Affected Individuals

On September 26, 2025, Business Integra notified 1 New Hampshire resident within the potentially affected population, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

13515559v1

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in complimentary identity protection services including 12 months of credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

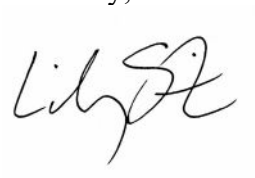
4. Steps Taken Relating to the Incident

Upon discovering this incident, in addition to taking the steps described above, Business Integra took steps to learn more about what happened and what information could have been affected. Business Integra has established a toll-free call center through Transunion to answer questions about the incident and address related concerns. Finally, Business Integra notified the potentially affected individuals and provided them with steps they can take to protect their personal information.

5. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,



Lindsey Smith
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter

Business Integra Technology Solutions
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1937

0000232

1_0000232

[redacted]

September 26, 2025

Subject: Notice of Data Breach

Dear [redacted]:

I am writing to inform you of a recent data security incident that may have affected your personal information. Business Integra Technology Solutions, Inc. ("Business Integra") the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On August 23, 2025, Business Integra experienced a network disruption and immediately began investigating with the assistance of independent cybersecurity experts. As a result of the investigation, we determined that certain files were potentially acquired without authorization. Business Integra then reviewed the files, and on September 11, 2025, we learned that your personal information was contained in the affected data. Please note that Business Integra has no evidence of the misuse, or attempted misuse, of your information.

What Information Was Involved. The information may have included: your name, Social Security number, driver's license, Passport number, and financial account information.

What We Are Doing. As soon as Business Integra discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future.

Additionally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to *https://bfs.cyberscout.com/activate* and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive

the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do. In addition to enrolling in the complimentary credit monitoring described above, you can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through Cyberscout by using the enrollment code provided above.

For More Information. Further information about how to protect your personal and protected health information appears on the following page. If you have questions or need assistance, please call 1-800-405-6108 Monday through Friday from 8:00 am- 8:00 pm Est, excluding holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Jacki Sabine
HR Manager
Business Integra Technology Solutions, Inc.
6550 Rock Spring Drive, Suite 600
Bethesda, MD 20817
(301) 474-9600 x 146

0000232

Steps You Can Take to Help Protect Your Personal 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 (the "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 www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. 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 www.annualcreditreport.com.

Security Freeze: 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.