BakerHostetler

Baker&Hostetler LLP
Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

June 24, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Integrity Data, Inc. ("Integrity"), and one or more of its clients, to notify you of a security incident involving three New Hampshire residents.[1]

Integrity is a payroll software company that offers payroll processing and human capital management services to clients in a variety of industries. To accomplish this function, Integrity receives from its clients necessary data about employees including certain types of personal information.

On June 5, 2020, Integrity began contacting clients that had provided it with personal information that was involved in an email phishing incident. The emails and/or attachments in the account with unauthorized access were sent to Integrity by Integrity's clients. Integrity has an internal policy to remove sensitive information when they receive it and to notify the sender that sending such information is a violation of Integrity's policy. The information relating to the New Hampshire residents was contained in one of a handful of emails that had not yet been removed under Integrity's policy. Integrity offered to provide notification to each client's individuals whose information was involved in the incident, as well as complimentary credit monitoring services, call center services, and required regulatory notifications. Integrity is now providing notice to individuals whose information was provided to it by a client who accepted Integrity's offer. Three

[1] This notice does not waive Integrity's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this incident.

of these individuals have been identified as New Hampshire residents and the information includes their name and Social Security number.

Integrity contacted its clients shortly after completing its forensic investigation into the email phishing incident that resulted in an unauthorized person gaining access to a support email account between April 22, 2020 and April 27, 2020. Upon learning of the incident, Integrity took measures to secure the email account, launched an internal investigation, and engaged a cybersecurity firm to assist in determining the nature and scope of the incident. While the investigation could not confirm that any emails or attachments were viewed by the unauthorized person, Integrity could not rule out that possibility. Accordingly, Integrity conducted a comprehensive search and review of the emails and attachments in the account.

Beginning June 24, 2020, Integrity is providing written notice to the New Hampshire residents pursuant to N.H. Rev. Stat. Ann. § 359-C:20, in substantially the same form as the enclosed letter. Integrity is offering the New Hampshire residents a complimentary one-year membership to credit monitoring and identity theft protection services through Kroll. Integrity has also established a dedicated toll-free call center where all individuals may obtain more information regarding the incident.

To further protect personal information, Integrity is implementing additional procedures to further strengthen their email security and are providing additional training to their employees regarding their policy of removing sensitive information from their systems when received via unsecured methods.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

David E. Kitchen
Partner

Enclosure

Integrity Data.

Your people. Our priority.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Integrity Data, Inc. is a payroll software company that allows companies to manage and streamline payroll processes. To accomplish this function, we receive necessary data about employees, including certain types of personal information. We place a high value on maintaining the integrity and security of the data we hold for our clients. Regrettably, we write to inform you that we identified and addressed a security incident that may have involved some of your information, which was provided to us in connection with the services we provide to [redacted]. This notice describes the incident, outlines the measures we have taken in response, and provides steps you can take.

On June 8, 2020, we notified [redacted] that we had identified suspicious activity within our support email account, a shared service account used by Integrity employees. Upon discovering the suspicious activity, we secured the account, launched an investigation to determine the nature and scope of the incident, and a professional information technology firm was engaged to assist. On May 5, 2020, the investigation determined that an unauthorized person accessed the support mailbox between April 22, 2020 and April 27, 2020. The investigation was unable to determine which emails and/or attachments were viewed by the unauthorized person, if any. We therefore reviewed the full contents of the account for personal information sent to this account and determined that an email or an attachment contained your information, including your name, Social Security number, and potentially your date of birth.

Although we cannot confirm your information was viewed, and have no indication that your information has been misused, we wanted to inform you of this incident and offer recommendations on ways to safeguard your information. We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. As an added precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **September 21, 2020** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

For more information on identity theft prevention and your complimentary one-year membership, please see the additional information provided in this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To help prevent similar incidents from happening in the future, we are implementing additional procedures to further strengthen our email security and are providing additional training to our employees regarding our policy of removing sensitive information from our systems when received via unsecured methods. If you have any questions, please call 1-844-958-2757, Monday through Friday from 8:00 A.M. through 5:30 P.M. Central Time.

Sincerely,

Thomas Franz
Director of Finance & IS

ELN-2369-0620

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You can contact Integrity Data by writing to them at 125 N. Kickapoo St., Lincoln, IL 62656 or by telephone at (217) 732-3737. You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.