Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 9, 2016

NOTICE OF POTENTIAL SECURITY INCIDENT

Dear John Sample,

LAZ Parking recently experienced a security incident involving certain personal information contained in files and records maintained by LAZ Parking in connection with your employment. We are providing this notice to inform you and other potentially affected employees of the incident and to call your attention to steps you can take to help protect yourself and your personal information. We sincerely apologize for any inconvenience or concern this may cause you and we assure you that we are doing everything we can to ensure that it will not happen again.

What Happened

On February 17, 2016, an unknown individual, impersonating a LAZ Parking executive, contacted a LAZ Parking employee by email and requested tax documentation pertaining to individuals employed by LAZ Parking during the 2015 calendar year. The LAZ Parking employee complied, believing the communication to be authentic, and sent a reply correspondence that included PDF copies of certain employees' 2015 Form W-2s. When these communications were brought to the attention of senior management after the reply correspondence had already been sent, it was determined that the request was fraudulent.

What Information Was Involved

Based on our internal investigation of the matter, we have determined that your 2015 Form W-2 was among those that were inadvertently disclosed, and that certain of your personal information may have been put at potential risk, including your first and last name, home address, social security number, and 2015 compensation data.

What We Are Doing

LAZ Parking takes the privacy and protection of its employees' personal information very seriously and we deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter in order to develop a better understanding of what had taken place and how. We are now in the process of reviewing our internal policies and data-management protocols and will be implementing enhanced security measures to help prevent this type of incident from recurring in the future. We have also reported the matter to law enforcement and plan to cooperate with appropriate authorities going forward.

To help protect you and your personal information, LAZ Parking is offering all potentially affected employees twenty-four (24) months of complimentary identity repair and protection services, including credit monitoring. See the reference materials included with this correspondence for further information, and be sure to note your redemption code, which you will need in order to complete the enrollment process: Redemption Code.

What You Can Do

Potentially affected employees can take the following steps to guard against identity theft and fraud:

- Register for the complimentary identity repair and protection services, provided by LAZ Parking at no cost to you, using the activation information included in the enclosed reference materials.

01-03-1-00

- Although employee financial account details were not affected by this incident, as a general precaution we recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed.
- Remain vigilant and continue to monitor your bank and credit card statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, call the bank that issued your credit or debit card immediately.
- Carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As part of the complimentary protection, you may discuss your concern with any of the three primary credit agencies—Equifax, Experian, and TransUnion (see enclosures for contact information).
- Place a "fraud alert" or "security freeze" on your credit file. Information about these options for your credit file, along with instructions for activating these options, can be found in the enclosed reference materials, or by contacting one of the three credit agencies noted above.
- Review the enclosed "Information about Identity Theft Protection" reference guide, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection.

Finally, we are asking all of our employees to remain attentive to any unusual inquiries concerning LAZ employee or customer data. If you receive a suspicious email, do NOT reply and immediately contact your manager for further instructions.

For More Information

Enclosed is a list of Frequently Asked Questions that provide additional information about the incident. We have also established a Call Center to assist you with any other questions or concerns you may have about this incident. The Call Center can be reached by dialing 855-731-6014 between 9:00 AM and 9:00 PM (Eastern Time), Monday through Saturday.

On behalf of the partners of LAZ, we sincerely regret the inconvenience and concerns caused by this incident. We are doing everything we can to minimize disruption for everyone involved.

Very truly yours,

Alan B. Lazowski
Chairman, CEO and Founder

LAZ Karp Associates, LLC
15 Lewis Street
Hartford, CT 06103

PROOF COPY

FAQs for LAZ Parking Employees

1. **What happened?**

   LAZ Parking recently experienced a security incident involving certain personal information contained in files and records maintained by LAZ Parking in connection with your employment.

   On February 17, 2016, an unknown individual, impersonating a LAZ Parking executive, contacted a LAZ Parking employee by email and requested tax documentation pertaining to individuals employed by LAZ Parking during the 2015 calendar year. The LAZ Parking employee complied, believing the communication to be authentic, and sent a reply correspondence that included PDF copies of certain employees' 2015 Form W-2s. When these communications were brought to the attention of senior management after the reply correspondence had already been sent, it was determined that the request was fraudulent.

   We took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter in order to develop a better understanding of what had taken place and how. We are now in the process of reviewing our internal policies and data-management protocols and will be implementing enhanced security measures to help prevent this type of incident from recurring in the future.

   We apologize for any inconvenience or concern caused by this incident.

2. **Was any of my financial account information or personnel file information exposed?**

   No. Aside from the information that is included on your 2015 Form W-2, no other personal or sensitive information was involved in this incident or otherwise put at potential risk.

3. **When did you discover this security incident?**

   LAZ Parking determined that the email request for employee-related tax documentation was fraudulent on February 17, 2016, shortly after the LAZ Parking employee sent the reply correspondence and then brought the communications to the attention of senior management.

4. **Why was there a delay between discovering the incident and notifying me that this happened?**

   Upon confirming the fraudulent email, LAZ Parking immediately initiated an internal investigation of the matter to determine, among other things, which of our employees may have been affected by the incident. Once we were able to successfully identify the population of potentially affected employees, we secured high-quality ID protection services for each of our employees whose information may have been put at risk and began to mobilize and coordinate internal and outside resources in order to provide this notice.

5. **Who is responsible for this incident?**

   Although we are continuing to work with law enforcement on this matter, at this time we do not have any details about the individuals that may be responsible for this incident and/or have access to your personal information.

6. **Was my information impacted by this incident?**

   If you are a current or former employee of LAZ Parking and were employed during the 2015 calendar year, your 2015 Form W-2 was among those that were inadvertently disclosed, and certain of your personal information may have been put at potential risk—including your first and last name, home address, social security number, and 2015 compensation data. Current and former employees that were not employed by LAZ Parking for any period of time between January 1, 2015 and December 31, 2015 were <u>not</u> affected by this incident.

7. **Was this incident reported to the police or other law enforcement authorities?**

   Yes, we have been in contact with appropriate law enforcement and will continue to cooperate with their ongoing investigation.

8. **What new security measures are being implemented to prevent this from happening in the future? What have you done to fix the problem?**

   After learning of the incident, we promptly took steps to investigate the incident and to ensure that no additional employee information may have been put at risk. We are currently reviewing our internal policies and data-management protocols and will be implementing enhanced security measures to help prevent this type of incident from recurring in the future, including by working to raise employee awareness on how to properly handle requests for sensitive information and how to recognize a potential "phishing scheme."

   As noted before, we have also reported the incident to law enforcement and will continue to cooperate with appropriate authorities going forward.

9. **What are you going to do to help employees who are impacted?**

LAZ Parking takes this matter very seriously. For all employees potentially affected by this incident, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this correspondence and you can use them at any time during the next 24 months:

1) *AllClear SECURE*: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 855-731-6014 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

2) *AllClear PRO*: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 855-731-6014 and using the redemption code included in the letter enclosed with these FAQs.

   Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

By way of further assistance, LAZ Parking will reimburse any potentially affected employees for out-of-pocket costs related to credit freeze placement, temporary lifting and/or removal of credit freeze, with supporting documentation of the expenses. Please submit any reimbursement request, with supporting documentation, through the usual expense reimbursement process and describe the expense as "Credit Freeze Cost."

In addition, we have also provided further suggestions on steps that you can take to help protect yourself and your personal information from misuse, which may be found in the "Information about Identity Theft Protection" reference guide that is included with this correspondence.

10. **What should I do to protect myself from fraud?**

First, we encourage all affected employees to activate the Identity Protection Services being provided to you by LAZ Parking for 24 months, free of charge. Refer to question 6 if you are unsure of whether you may have been affected by this incident.

We also recommend that you carefully check credit reports for accounts or inquiries you do not recognize. If you see that you do not understand, call the credit agency immediately. Contact information for the three national credit reporting agencies may be found in the "Information about Identity Theft Protection" reference guide that is included with this correspondence. If you find any suspicious activity on the credit reports which you do not recognize or which does not reflect your personal account activity, consider calling your local police to file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up credit records.

Because this incident involved your social security number and other tax-related information that was included in your 2015 Form W-2, ***we strongly encourage you to file your tax return for the 2015 tax year as soon as possible in order to help prevent tax-related identity theft and/or fraud***. If you learn that a tax return has already been filed using your personal information, or if you otherwise suspect that you may have been a victim of tax fraud, you should take the following steps:

- Immediately contact the IRS to report and receive specialized assistance concerning any tax-related misuse of your personal information, by calling at 1-800-908-4490.
- Promptly respond to any IRS notice by calling the number provided or, if instructed, by visiting www.IDVerify.irs.gov.
- If your efiled return is rejected because of a duplicate filing under your social security number, immediately report the false filing to the IRS and complete IRS Form 14039 (Identity Theft Affidavit), which is available on the IRS.gov website. (Note you must continue to pay your taxes and file your tax return, even if you must do so by paper.)
- Contact one of the three national credit reporting agencies to place a "fraud alert" on your credit records, as detailed in the "Information about Identity Theft Protection" reference guide that is included with this correspondence.

Finally, we also recommend that all potentially affected employees review the enclosed "Information about Identity Theft Protection" reference guide, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection. The IRS has also published information about tax-related identity theft and fraud, which you are encouraged to review by visiting www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

11. **I might choose to put a "credit freeze" on my accounts, as described in the Information About Identity Theft Protection reference guide. Will LAZ Parking reimburse me if I am required to incur any fees in doing so?**

    LAZ Parking will reimburse any affected employees for out-of-pocket costs related to credit freeze placement, temporary lifting and/or removal, with supporting documentation of the expenses. Please submit any reimbursement request, with supporting documentation through the usual expense reimbursement process and describe the expense as "Credit Freeze Cost."

12. **I want to enroll for the AllClear ID identity repair and protection services. How do I do that?**

    AllClear ID's identity repair assistance is available to you automatically and does not require you to take additional steps to activate your coverage. If a problem arises, simply call 855-731-6014 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

    However, in order to take full advantage of the complimentary identity repair and protection services, including credit monitoring, you will need to enroll and provide your personal information to AllClear ID, which you may do online at enroll.allclearid.com or by phone by calling 855-731-6014 using the redemption code included in the letter enclosed with these FAQs.

    Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

13. **What should I do if I receive an email that I am not sure about?**

    If you receive any suspicious emails at any time, do NOT reply and please immediately contact your manager for further instructions.

If you would like additional information about this incident, please contact the call center at 855-731-6014 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Saturday.

Proof Copy

Information about Identity Theft Protection

Identity Theft Protection: As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this correspondence and you can use them at any time during the next 24 months:

1) AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 855-731-6014 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

2) AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 855-731-6014 using the following redemption code: Redemption Code. *Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.*

By way of further assistance, LAZ Parking will reimburse any potentially affected employees for out-of-pocket costs related to credit freeze placement, temporary lifting and/or removal of credit freeze, with supporting documentation of the expenses. Please submit any reimbursement request, with supporting documentation, through the usual expense reimbursement process and describe the expense as "Credit Freeze Cost."

Additional Suggestions: We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that 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 at least 90 days. At the end of 90 days, you can contact the credit reporting agency to place another 90 day fraud alert on your credit report. You also may have a free extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof (generally, a police report is required). An extended fraud alert stays on your credit report for seven years. *You can place a fraud alert on your credit report at any time by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.*

Credit Freezes: In addition, you may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. As the instructions for how to establish a credit freeze vary by state, please contact the major credit reporting companies as specified below to find out more information.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or any of the credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts: P.O. Box 740256, Atlanta, GA 30374
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872