Representing Management Exclusively in Workplace Law and Related Litigation

jackson lewis.

Jackson Lewis P.C.
220 Headquarters Plaza
East Tower, 7th Floor
Morristown, NJ 07960-6834
Tel 973 538-6890
Fax 973 540-9015
www.jacksonlewis.com
Richard J. Cino - Managing Principal

ALBANY, NY	GREENVILLE, SC	MONMOUTH COUNTY, NJ	RALEIGH, NC
ALBUQUERQUE, NM	HARTFORD, CT	MORRISTOWN, NJ	RAPID CITY, SD
ATLANTA, GA	HONOLULU, HI*	NEW ORLEANS, LA	RICHMOND, VA
AUSTIN, TX	HOUSTON, TX	NEW YORK, NY	SACRAMENTO, CA
BALTIMORE, MD	INDIANAPOLIS, IN	NORFOLK, VA	SALT LAKE CITY, UT
BIRMINGHAM, AL	JACKSONVILLE, FL	OMAHA, NE	SAN DIEGO, CA
BOSTON, MA	KANSAS CITY REGION	ORANGE COUNTY, CA	SAN FRANCISCO, CA
CHICAGO, IL	LAS VEGAS, NV	ORLANDO, FL	SAN JUAN, PR
CINCINNATI, OH	LONG ISLAND, NY	PHILADELPHIA, PA	SEATTLE, WA
CLEVELAND, OH	LOS ANGELES, CA	PHOENIX, AZ	ST. LOUIS, MO
DALLAS, TX	MADISON, WI	PITTSBURGH, PA	TAMPA, FL
DAYTON, OH	MEMPHIS, TN	PORTLAND, OR	WASHINGTON, DC REGION
DENVER, CO	MIAMI, FL	PORTSMOUTH, NH	WHITE PLAINS, NY
DETROIT, MI	MILWAUKEE, WI	PROVIDENCE, RI	
GRAND RAPIDS, MI	MINNEAPOLIS, MN		

*through an affiliation with Jackson Lewis P.C., a Law Corporation

JASON C. GAVEJIAN
jason.gavejian@jacksonlewis.com

April 15, 2019

VIA OVERNIGHT MAIL

Office of Attorney General
Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[2]

Dear Attorney General:

Please be advised that on March 14, 2019, our client, Lakeland Finance, LLC dba WorldStrides ("WorldStrides"), learned that personal information of state residents may have been subject to unauthorized access or acquisition as the result of a cyber-attack in which unauthorized users utilized phishing emails to gain access to some employee email accounts. Based on the investigation, it appears the attack occurred between October 15, 2018 and November 21, 2018. The data elements involved may have included name, birth date, Social Security number, driver's license number, passport number, state identification number, financial account information, and/or very general medical or health information.

Immediately upon discovering the unauthorized access, WorldStrides commenced an investigation to determine the scope of this incident and identify those potentially affected. WorldStrides' remediation steps included providing immediate notice of the incident to those employees whose accounts were discovered to have been accessed. WorldStrides worked with its information technology team to secure and scan its systems for malicious activity in an effort to ensure the attack did not result in any additional exposure to personal information. WorldStrides also retained a third party forensic vendor to determine what information may have been accessed. The forensic vendor determined that the unauthorized actor gained access to some WorldStrides employee email accounts, but was unable to determine what, if any, information contained within the accounts was accessed or exfiltrated as a result of the unauthorized access. Thus, WorldStrides engaged a firm to perform data mining on each of the

[2] Please note that by providing this letter WorldStrides is not agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

impacted email accounts to determine whether they contained any personal information. Based on the results of the data mining, it appears that 478 individuals could have been affected, including 1 New Hampshire resident. In light of this incident, WorldStrides plans to begin notifying individuals in the next week. WorldStrides will also provide one year of free credit monitoring to all affected individuals. A draft copy of the notification that will be sent is enclosed with this letter.

As set forth in the enclosed letter, WorldStrides has taken numerous steps to protect the security of the personal information of all individuals. In addition to continuing to monitor this situation, WorldStrides is reexamining its current privacy and data security policies and procedures to find ways of reducing the risk of future data incidents. WorldStrides is also reviewing its technical security policies and procedures and making improvements where it can to minimize the chances of this happening again. Should WorldStrides become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS P.C.

Jason Gavejian II

Jason C. Gavejian

Encl.

4838-6614-2612, v. 1

Return Mail Processing Center
P.O. Box 9349
Dublin, OH 43017

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

April 17, 2019

Notice of Data Breach

Dear <<Name 1>>:

Lakeland Finance, LLC dba WorldStrides ("WorldStrides") recently learned that some of your personal information may have been subject to unauthorized access or acquisition. If you are not a current or former WorldStrides employee, this information may have been maintained by WorldStrides in connection with a trip you participated in and which was run by WorldStrides. While we are not aware of any misuse of your information, we apologize for any inconvenience this may cause you and assure you that we have worked diligently to resolve this incident and continue to deploy measures to avoid these types of incidents from occurring in the future. Below you will also find instructions and a code redeemable for one year of credit monitoring with TransUnion.

What Happened
On March 14, 2019, WorldStrides discovered that your personal information may have been accessible to an unauthorized actor as the result of a cyberattack. Based on the investigation, it appears the attack occurred between October 15, 2018 and November 21, 2018.

What Information Was Involved
The personal information subject to this incident may have included your name, birth date, Social Security number, driver's license number, passport number, state identification number, financial account information, and/or very general medical or health information.

What We Are Doing
Immediately upon discovering the intrusion, we commenced an investigation to determine the scope of this incident and identify those affected. We worked with our information technology team and hired third party forensic experts to conduct a thorough scan of our systems in an effort to ensure the incident did not result in any additional exposure to personal information, and took steps to confirm the integrity of WorldStrides's electronic systems. We also worked with third party experts to determine what information may have been at risk of unauthorized access. We have reported this incident to the Federal Bureau of Investigation ("FBI"). This communication was not delayed at the request of law enforcement.

As an added precaution, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. To receive these services you must enroll by <<Enrollment Deadline>>.

- To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following Activation Code:

  <<Insert Unique 12-letter Activation Code>>

- Then follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code [CODE] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

- Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We treat all personal information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Unauthorized access to personal information and similar incidents are difficult to prevent in all instances; however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

What You Can Do

We are sending this advisory to you and other individuals to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. In addition to enrolling in the credit monitoring service mentioned above, set forth below are steps you can take to protect your identity, credit and personal information.

For More Information

If you have questions or concerns, you should call (855) 821-6789 from 9 am to 9 pm Eastern. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

Signatory Name
Signatory Title

PLEASE SEE ATTACHED FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for one year.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com

   - Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Obtain a free copy of your credit report by going to www.annualcreditreport.com.

2. Please review all bills and credit card statements closely to determine whether you have been charged for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes delay their use of stolen personal information.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police and/or your state Attorney General. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

4. *For Maryland Residents*: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.

5. *For North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com.

6. *For Rhode Island Residents*: The contact information for the Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is 535.

WorldStrides®

Return Mail Processing Center
P.O. Box 9349
Dublin, OH 43017

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

April 17, 2019

Notice of Data Breach

Dear <<Name 1>>:

Lakeland Finance, LLC dba WorldStrides ("WorldStrides") recently learned that some of your minor's personal information may have been subject to unauthorized access or acquisition. If your minor is not a current or former WorldStrides employee, this information may have been maintained by WorldStrides in connection with a trip your minor participated in and which was run by WorldStrides. While we are not aware of any misuse of your minor's information, we apologize for any inconvenience this may cause you and assure you that we have worked diligently to resolve this incident and continue to deploy measures to avoid these types of incidents from occurring in the future. Below you will also find instructions and information about minor/child identity theft.

What Happened
On March 14, 2019, WorldStrides discovered that your minor's personal information may have been accessible to an unauthorized actor as the result of a cyberattack. Based on the investigation, it appears the attack occurred between October 15, 2018 and November 21, 2018.

What Information Was Involved
The personal information subject to this incident may have included your minor's name, birth date, Social Security number, driver's license number, passport number, state identification number, financial account information, and/or very general medical or health information.

What We Are Doing
Immediately upon discovering the intrusion, we commenced an investigation to determine the scope of this incident and identify those affected. We worked with our information technology team and hired third party forensic experts to conduct a thorough scan of our systems in an effort to ensure the incident did not result in any additional exposure to personal information, and took steps to confirm the integrity of WorldStrides's electronic systems. We also worked with third party experts to determine what information may have been at risk of unauthorized access. We have reported this incident to the Federal Bureau of Investigation ("FBI"). This communication was not delayed at the request of law enforcement.

Each of the three national credit-reporting agencies provide services and information regarding minor/child identity theft. Those resources may be found online at:

- TransUnion: https://www.transunion.com/fraud-victim-resource/child-identity-theft
- Experian: https://www.experian.com/blogs/ask-experian/how-can-you-check-your-minor-childs-credit-report-if-you-suspect-illegal-activity/
- Equifax: https://www.equifax.com/personal/education/identity-theft/child-identity-theft/

We treat all personal information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Unauthorized access to personal information and similar incidents are difficult to prevent in all instances; however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

What You Can Do

We are sending this advisory to you and other individuals to make you aware of this incident so that you can take steps to protect your minor and minimize the possibility of misuse of your minor's information. In addition to minor/child identity theft services and information available from the three national credit-reporting agencies, set forth below are steps you can take to protect your minor's identity, credit and personal information.

For More Information

If you have questions or concerns, you should call (855) 821-6789 from 9 am to 9 pm Eastern. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

Signatory Name
Signatory Title

PLEASE SEE ATTACHED FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your minor's personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
   - Add a fraud alert statement to your minor's credit file (if one exists) at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your minor's report as well as requests that they contact you prior to establishing any accounts in your minor's name. Once the fraud alert is added to your minor's credit report, all creditors should contact you prior to establishing any account in your minor's name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a fraud alert on your minor's credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your minor's credit file for one year.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com

   - Place a "security freeze" on your minor's credit account (if one exists). This means that your minor's credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your minor's account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies.
   - Remove your minor's name from mailing lists of pre-approved offers of credit for approximately six months.
   - Obtain a free copy of your minor's credit report (if one exists) by going to www.annualcreditreport.com.

   Note that the services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

2. Please review all bills and credit card statements closely to determine whether your minor has been charged for items your minor did not contract for or purchase. Review all of your minor's bank account statements frequently for checks, purchases, or deductions not made by your minor. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes delay their use of stolen personal information.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that your minor is the victim of identity theft, you should contact local police and/or your state Attorney General. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

4. *For Maryland Residents*: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.

5. *For North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com.

6. *For Rhode Island Residents*: The contact information for the Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is 535.