Winget | Spadafora | Schwartzberg | LLP

PENNSYLVANIA:
1528 Walnut Street
Suite 1502
Philadelphia, PA 19102
T 215.433.1500
F 215.433.1501
Wertman.J@WSSLLP.com

January 6, 2021

VIA FIRST CLASS MAIL
NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

RE: Data Incident Notification
UFCW Local 1776

To Whom It May Concern:

Let this letter serve as the notification requirement pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b) pertaining to a data incident involving two (2) New Hampshire residents as to the above referenced entity located in Pennsylvania. The data incident occurred on the computer system of the above referenced entity and involved New Hampshire residents whose information was originally sourced by the Pennsylvania Liquor Control Board and maintained on the above referenced entity's system for union related purposes. There is no indication that there has been any breach of the Pennsylvania Liquor Control Board's computer system. This letter follows the results of a forensic investigation that was recently completed. A sample copy of the notification letter is enclosed.

On or about September 11, 2020, we learned that there was potentially unauthorized access from a foreign IP system to union employee e-mails which contained certain limited information as to certain individuals from approximately July 14, 2020-August 12, 2020. An in depth analysis of the union employee emails, to determine which individuals were affected, was completed on or about November 4, 2020. Analysis was completed on December 30, 2020, in order to verify contact information for this notice. Prior to December 30, 2020, neither the addresses of the affected individuals nor contact information for the affected individuals was known. The investigation is now complete but, unfortunately, the forensic IT firm cannot determine which files, if any, were actually accessed.

The information included the following information full name and Social Security Number. The information was contained in an excel file wherein the Social Security Numbers were hidden from view, subject to reformatting. Out of an abundance of caution, everyone whose information was potentially accessible is being notified.

We have no way of knowing which individuals' information may have been accessed, so all individuals are being notified in an overabundance of caution. In addition, we are providing complimentary credit monitoring services through IDX to all affected persons for a period of one year. Notices are being sent beginning on January 5, 2021 through IDX.

Should you have any additional questions, please do not hesitate to contact counsel listed below.

Sincerely,

/s/ Joel Wertman

Joel Wertman, Esq.

UFCW Local 1776
C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
833-905-3226
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 5, 2021

Notice of Data Incident

Dear «First_Name» «Last_Name»,

Please allow this letter to notify you of a data incident involving some of your personal information. We take the privacy of your information very seriously and recommend that you closely review the information provided in this letter for steps that you may take to protect yourself against the potential misuse of information.

What Happened?

On or about September 11, 2020, we learned that there was potentially unauthorized access from a foreign IP system to union employee e-mails which contained certain limited information as to certain individuals from approximately July 14, 2020-August 12, 2020. An in depth analysis of the union employee emails, to determine which individuals were affected, was completed on or about November 4, 2020. Analysis was completed on December 30, 2020, in order to verify your contact information for this notice. The investigation is now complete but, unfortunately, the forensic IT firm cannot determine which files, if any, were actually accessed. Out of an abundance of caution, I am notifying everyone whose information was potentially accessible.

What Information Was Involved?

If you are a member of the union, the information may have included the following information: full name, address, Social Security Number, and government identification number.

If you are not a member of the union, the information may have included the following information: full name, address, Social Security Number, and government identification number.

What We are Doing

Cyber-attacks on email continue to increase and evolve. For this reason and to help prevent this type of incident in the future, we are continuously enhancing our data security procedures. In addition, we have worked diligently with counsel and third party vendors of identity protection services to resolve this matter and protect your personal information. Likewise, we are currently in the process of communicating with the appropriate law enforcement departments, where appropriate.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a

$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 833-905-3226 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 3, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 833-905-3226 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Wendell W. Young, IV
President

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 833-905-3226 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.