15175

May [x], 2019

NOTICE OF DATA BREACH

[First Name] [Last Name]
[Street Address]
[City], [State] [Zip Code]

Dear [Mr./Mrs./Ms.] [Last Name],

We are writing to inform you that one of our vendor's employees may have obtained and used your debit or credit card information without authorization. Once we became aware of the situation, we worked with the vendor to terminate the individual's access to your information.

The protection of personal information is a matter we take seriously, and we recommend that you review this letter for steps you can take to safeguard your information.

What Happened?

The vendor recently told us that its employee (who we understand has since been terminated) may have accessed a limited number of our customers' debit or credit card information from approximately April 24 to April 26, 2019 and, in some cases, may have made fraudulent purchases using that information. The vendor was unable to determine whether the employee actually made fraudulent purchases with your information, but we are notifying you out of an abundance of caution.

What Information Was Involved?

Based on the vendor's investigation, the vendor's employee may have accessed your name and debit/credit card information.

What We Are Doing

As soon as we were informed of the issue, we worked with the vendor to investigate the incident and protect your information.

What You Can Do

As part of our efforts to assist you, we have retained Experian, a specialist in identity theft protection, to provide you with two years of credit monitoring and identity theft services, free of charge. You can enroll in the program by following the directions below.

- Ensure that you **enroll by**: [Activation Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website (https://www.experianidworks.com/3bplus) to enroll.
- Provide the following **activation code**: [Activation Code]

- Remember your **engagement number**: [Engagement Number]

Please keep this letter; you will need the personal activation code it contains in order to register for services. The enclosed information guide provides additional steps you can take to further protect your information.

For More Information

We apologize for any inconvenience this issue may cause you. If you have any questions regarding this issue or you would like further information or assistance, please do not hesitate to call 1-877-262-2949 between the hours of 7 a.m. and 10 p.m. Eastern Standard Time, Monday through Friday, to speak with someone who can help.

Sincerely,

Ron Zanders
Vice President – Vendor Relations

Additional Information

What You Can Do

Remain Vigilant

We recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are reported timely.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement authorities, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently, and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies (Equifax, Experian, and TransUnion) to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you can obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay

your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. Please be aware, however, that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each consumer reporting company.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

You may contact the nationwide consumer reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)

(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above.

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
http://www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above.