BakerHostetler

Baker&Hostetler LLP
312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074
T 513.929.3400
F 513.929.0303
www.bakerlaw.com
Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

August 30, 2019

VIA OVERNIGHT MAIL

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

Re: Supplemental Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, TALX Corporation ("TALX"), to provide additional information about a security incident previously reported to your office. TALX provides this notice on behalf of its customer, CVS Health. TALX's headquarters are located at 11432 Lackland Road, St. Louis, Missouri 63146.

CVS Health has contracted with TALX, a wholly owned subsidiary of Equifax Inc., to provide payroll-related services that CVS Health employees are able to access through www.mytaxform.com ("online portal"). In 2017, TALX or CVS Health notified your office of an incident in which an unauthorized person or persons reset the user PIN (the user password to access the online portal) and then accessed the account of certain CVS Health employees. Upon learning of this, TALX promptly conducted an investigation and determined that the unauthorized person(s) were able to successfully answer the challenge questions needed to reset the employees' PINs through the Knowledge-Based Authentication ("KBA") security option on the online portal.[1] TALX has no indication that either CVS Health or TALX was the source of any of the information used to reset the PINs. TALX and/or CVS Health provided notice to the individuals involved.

On July 8, 2019, TALX discovered that the unauthorized person(s) accessed the account of one additional CVS Health employee residing in New Hampshire. This is not new activity but is additional activity from the prior incident that was recently discovered. The date of access was

[1] KBA is an authentication method under which where a user must successfully answer a series of personal questions derived from that user's credit file.

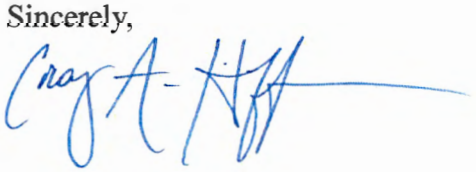
December 10, 2016. The unauthorized individual(s) may have accessed an electronic copy of the 2015 W-2 form for the CVS Health employee.

CVS Health is notifying this resident via U.S. mail using a template drafted by TALX. A copy of the notification letter is attached hereto. The letter offers the resident 24 months of ID Patrol identity protection service at no cost to the resident. It also advises the resident to remain vigilant, to review his financial account statements for suspicious activity, and to report this incident to the Internal Revenue Service and the state tax agency as soon as possible. Lastly, it provides a telephone number for the resident to call with any questions he may have.

Although TALX has no indication that either CVS Health or TALX was the source of the information used to reset the PIN, TALX has implemented additional authentication and security measures to help prevent a recurrence of this type of incident. In 2017, TALX altered its KBA to increase the difficulty of passing KBA. TALX also implemented iOvation's fraud prevention tool to block known suspicious IP addresses as well as connections with other suspicious characteristics. In addition, TALX worked with CVS Health to alter the authentication methods used by CVS Health's employees. Later in 2017, TALX instituted a new authentication platform requiring multi-factor authentication.

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

Sincerely,



Craig A. Hoffman
Partner

Attachment

[Insert Company Logo / Name]

___ __, 2019

NAME
ADDRESS
CITY, STATE, ZIP

Dear _____:

We take the protection and proper use of your information very seriously. We are writing to tell you about an incident that may have resulted in the unauthorized access to an electronic copy of your <<TaxForm>> for tax year <<TaxFormYear1>>, <<TaxFormYear2>>. This notice explains the incident, measures we have taken, and additional steps you can take.

What Happened

CVS Health has contracted with Talx Corporation ("TALX"), a wholly owned subsidiary of Equifax Inc., to provide payroll-related services that you are able to access through www.mytaxform.com ("online portal"). We recently discovered that on <<date>>, an unauthorized person reset the user PINs (the user password to access the online portal) and then accessed the accounts of certain employees, including your account. Upon learning of this, TALX promptly took steps to understand how the access occurred and determined that the unauthorized person was able to successfully answer the challenge questions needed to reset the PINs. We have no indication that either CVS Health or TALX was the source of any of the information used to reset the PINs.

What Information Was Involved

An unauthorized individual may have accessed an electronic copy of your <<TaxForm>> for tax year <<TaxFormYear1>>, <<TaxFormYear2>>.

What We Are Doing

TALX has implemented additional authentication and security measures to help prevent a recurrence of this type of incident.

In addition, TALX is offering you 24 months of ID Patrol identity protection service at no cost to you. This service is explained further in the materials enclosed with this letter. To take advantage of this service, please follow the instructions in those materials.

What You Can Do

Because your tax form may have been accessed by an unauthorized individual, it is possible that a fraudulent tax return could be filed in your name. Therefore, we strongly recommend that you contact the Internal Revenue Service and your state tax agency as soon as possible to report this incident.

> Internal Revenue Service (IRS): You may contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. The IRS may request that you file IRS Form 14039 (which is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf). For additional information from the IRS about identity theft, you may visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.
>
> State Tax Agencies: Information on how to contact your state tax agency may be found by going to http://www.taxadmin.org/state-tax-agencies.

Finally, we urge you to enroll in the ID Patrol identity protection service being provided by TALX. Even if you choose not to enroll in the ID Patrol identity protection service, there are other steps you can take to help protect yourself. Please see the information in the "Identity Theft Prevention Tips" attachment about how you can obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report.

For More Information

We deeply regret that this incident occurred and are committed to ensuring that your personal information remains protected. If you have any questions, please call [number].

Sincerely,

CVS Health

Attachments: Identity Theft Prevention Tips
ID Patrol Offer and Information

Identity Theft Prevention Tips

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: There are two types of 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 (1) 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

ID Patrol Offer and Information

We have partnered with Equifax® to provide its ID Patrol identity theft protection product for 24 months at no charge to you. Information about ID Patrol, your personal Activation Code and enrollment instructions follow:

ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report
- Up to $1 million in identity theft insurance with $0 deductible

Please visit www.myservices.equifax.com/patrol for more information and to enroll for ID Patrol.

Your Activation Code is [XXXXX]. You must use this Activation Code to activate the product by [ ]. Please note that this Activation Code is non-transferable.

Coverage under ID Patrol will expire 24 months from the date you activate your code by enrolling for ID Patrol online.

ENROLLMENT TIPS:

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link!)**
2. Enter the Activation Code provided above and click the "Submit" button
3. The platform will walk you through the enrollment. Please enter the information requested and click the Continue button to step through the account setup screens
4. The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button
5. You will see an order confirmation page and you can click View My Product to access the product features
6. You will receive a confirmation email

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service (877-474-8273) to assist you in understanding the content of your Equifax credit information and to provide personalized identity theft victim assistance and assistance in initiating an investigation of inaccurate information.