15974

Appendix[1]

After detecting unauthorized activity on some of its payment processing systems on July 29, 2019, Hy-Vee immediately began an investigation and leading cybersecurity firms were engaged to assist. On August 14, 2019, Hy-Vee posted a message on its website and released a press release notifying its customers of the investigation. By October 1, 2019, findings from the investigation were available to accurately identify the Hy-Vee locations and specific timeframes involved in this incident.

The investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale ("POS") devices at certain Hy-Vee fuel pumps, drive-thru coffee shops, and restaurants (which include Hy-Vee Market Grilles, Hy-Vee Market Grille Expresses and the Wahlburgers locations that Hy-Vee owns and operates, as well as the cafeteria at Hy-Vee's West Des Moines corporate office). The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card as it was being routed through the POS device. However, for some locations, the malware was not present on all POS devices at the location, and it appears that the malware did not copy data from all of the payment cards used during the period that it was present on a given POS device. There is no indication that other customer information was accessed.

The specific timeframes when data from cards used at these locations involved may have been accessed vary by location over the general timeframe beginning December 14, 2018 to July 29, 2019 for fuel pumps and beginning January 15, 2019 to July 29, 2019 for restaurants and drive-thru coffee shops. There are six locations where access to card data may have started as early as November 9, 2018 and one location where access to card data may have continued through August 2, 2019.

Payment card transactions were not involved at Hy-Vee's front-end checkout lanes; inside convenience stores; pharmacies; customer service counters; wine & spirits locations; floral departments; clinics; and all other food service areas which utilize point-to-point encryption technology, as well as transactions processed through Aisles Online.

On October 3, 2019, two days after identifying the locations and timeframes involved in the incident, Hy-Vee provided substitute notice of the incident by posting an updated website message and issuing a press release with findings from the investigation. A list of the locations involved and their specific timeframes was posted on the Hy-Vee website message. Notification was not provided to your office at that time because none of the locations involved are in Massachusetts and our investigation had not yet identified Massachusetts residents whose information was involved in the incident.

Since providing substitute notice, Hy-Vee has been diligently working to identify those customers that used their payment card at a location involved during that location's specific timeframe and for whom Hy-Vee has a mailing address or email address via Hy-Vee's Fuel Saver rewards program. Now that Hy-Vee has completed the identification and matching process, Hy-

[1] This notice is not, and does not constitute, a waiver of Hy-Vee's objection that Massachusetts lacks personal jurisdiction over it regarding any claims related to this data security incident.

Vee is beginning to send notification letters today via First Class Mail to 40 Massachusetts residents in accordance with Mass. Gen. Laws Ann. Ch. 93H § 3. For individuals identified as having used a payment card at one of the locations involved during the location's specific timeframe and for whom Hy-Vee does not have a mailing address, Hy-Vee is emailing notifications to individuals for whom Hy-Vee has an email address. However, Hy-Vee does not have a mailing address or email address for all individuals that may have used a payment card at one of the locations involved during the location's specific timeframe, which is why Hy-Vee provided substitute notice on October 3, 2019. Enclosed is a sample copy of the letter. Hy-Vee also established a dedicated call center that customers can call with related questions.

Hy-Vee has removed the malware and implemented enhanced security measures and continues to work with cybersecurity experts to evaluate additional ways to enhance the security of payment card data. In addition, Hy-Vee continues to support law enforcement's investigation and is working with the payment card networks so that the card issuers can be made aware and initiate heightened monitoring.

Hy-Vee
EMPLOYEE OWNED

15974

TI PI 0000035 **********SNGLP

[redacted]

October 31, 2019

Dear [redacted]:

Hy-Vee, Inc. values the relationship we have with our customers and understands the importance of protecting payment card information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your payment card information, including your name, payment card number ending in [redacted], card expiration date, and internal verification code.

It is always advisable to review your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the following page for information on additional steps you may take.

During the investigation, we removed the malware and implemented enhanced security measures. We continue to work with cybersecurity experts to evaluate additional ways to enhance the security of payment card data at our locations. In addition, we continue to support law enforcement's investigation and are working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring.

Hy-Vee regrets any inconvenience or concern this may have caused. If you have additional questions, you can visit www.hy-vee.com/paymentcardincident or call 833-967-1091, Monday through Friday, between the hours of 8 a.m. and 8 p.m. Central Time.

Sincerely,

Matt Ludwig
Executive Vice President,
Business Innovation,
Chief Digital Officer
Hy-Vee, Inc.

ADDITIONAL STEPS YOU CAN TAKE

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 free annual 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

You may contact and obtain information from your state attorney general at:

- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Please note that pursuant to Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

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 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 personal identification number ("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 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 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.