BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

October 3, 2019

VIA E-MAIL CONSUMER@AG.IOWA.GOV

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Incident Notification

Dear Sir or Madam:

Hy-Vee, Inc. ("Hy-Vee") understands the importance of protecting the payment card information of its customers. 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 issued 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.

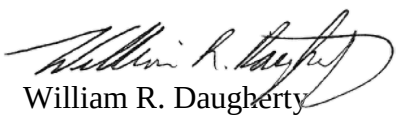
Payment card transactions were not involved at these locations: Hy-Vee's front-end checkout lanes; inside convenience stores; pharmacies; customer service counters; wine & spirits locations; floral departments; clinics; and all other food service areas which utilize point-to-point encryption technology,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

Hy-Vee does not have sufficient information to determine the name and mailing addresses of all individuals that used their cards at the Hy-Vee locations involved. Hy-Vee, therefore, is unable to identify the number of Iowa residents that used a card during the timeframe of this incident. Therefore, pursuant to Iowa Code Ann. § 715C.2, Hy-Vee is providing substitute notification to Iowa residents who may have used their payment cards at a Hy-Vee location involved by issuing a press release and posting an updated statement on its website today, October 3, 2019. A copy of the press release and website message are enclosed. A list of the locations involved in Iowa is available on the Hy-Vee website message. Hy-Vee also established a dedicated call center that customers can call with related questions. Notification is being provided without unreasonable delay. Lastly, Hy-Vee is diligently working to identify those customers that used their card at a location involved during that location's specific timeframe and for whom Hy-Vee has a mailing address or email address. A letter or email will be sent to those individuals in accordance with Iowa Code §715C.2.

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 banks that issue payment cards can be made aware and initiate heightened monitoring.

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

Sincerely,



William R. Daugherty
Partner

Enclosures

Website Notice

Will appear on: www.hy-vee.com/paymentcardincident

Hy-Vee Reports Findings from Investigation of Payment Card Data Incident

Hy-Vee is providing additional information about the payment card incident that we first reported on August 14, 2019. This following information further explains the incident, the measures we have taken, and some steps you can take in response.

After detecting unauthorized activity on some of our payment processing systems on July 29, 2019, we immediately began an investigation and leading cybersecurity firms were engaged to assist. We also notified federal law enforcement and the payment card networks.

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 our 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. A list of the locations involved and specific timeframes is available here. For those customers Hy-Vee can identify as having used their card at a location involved during that location's specific timeframe and for whom Hy-Vee has a mailing address or email address, Hy-Vee will be mailing them a letter or sending them an email.

Payment card transactions were not involved at our 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.

During the investigation, we removed the malware and implemented enhanced security measures, and we continue to work with cybersecurity experts to evaluate additional ways to enhance the security of payment card data. 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.

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 click here for information on additional steps you may take.

If you have additional questions, you can call 833-967-1091 Monday through Friday between the hours of 8:00 a.m. and 8:00 p.m. CT.

Additional Information

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

Press Release

Media contact:
Tina Potthoff
Senior Vice President, Communications
(515) 559-5770 – office
(515) 975-9211 – cell
tpotthoff@hy-vee.com

Hy-Vee Reports Findings from Investigation of Payment Card Data Incident

WEST DES MOINES, Iowa (Oct. 3, 2019) – See below for a statement from Hy-Vee, Inc. providing additional information about the payment card incident that Hy-Vee first reported on August 14, 2019:

Hy-Vee is providing additional information about the payment card incident that we first reported on August 14, 2019. This following information further explains the incident, the measures we have taken, and some steps you can take in response.

After detecting unauthorized activity on some of our payment processing systems on July 29, 2019, we immediately began an investigation and leading cybersecurity firms were engaged to assist. We also notified federal law enforcement and the payment card networks.

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 our 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.

A list of the locations involved and specific timeframes is available at www.hy-vee.com/paymentcardincident*. The site also provides information about the incident and additional steps customers may take. For those customers Hy-Vee can identify as having used their card at a location involved during that location's specific timeframe and for whom Hy-Vee has a mailing address or email address, Hy-Vee will be mailing them a letter or sending them an email.*

Payment card transactions were not involved at our 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.

During the investigation, we removed the malware and implemented enhanced security measures, and we continue to work with cybersecurity experts to evaluate additional ways to enhance the security of payment card data. 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.

It is always advisable for customers to review their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to their 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 the payment card.

For more information, please visit www.hy-vee.com/paymentcardincident.

ABOUT HY-VEE, INC.

Hy-Vee, Inc. is an employee-owned corporation operating more than 260 retail stores across eight Midwestern states with sales of $10 billion annually. The supermarket chain is synonymous with quality, variety, convenience, healthy lifestyles, culinary expertise and superior customer service. Hy-Vee ranks in the Top 10 Most Trusted Brands and has been named one of America's Top 5 favorite grocery stores. The company's more than 80,000 employees provide "A Helpful Smile in Every Aisle" to customers every day. For additional information, visit www.hy-vee.com.