



T251 P1 0070000 \*\*\*\*\*AUTO\*\*5-DIGIT 68130

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 information. This notice 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. Our records show that your Hy-Vee Fuel Saver card was used when making a purchase with a payment card(s) ending in [REDACTED] at a location involved during the location’s specific timeframe. A list of the locations involved and specific timeframes is available at [www.hy-vee.com/paymentcardincident](http://www.hy-vee.com/paymentcardincident).

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. 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.

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.

Hy-Vee regrets any inconvenience or concern this may have caused. If you have additional questions, you can visit [www.hy-vee.com/paymentcardincident](http://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,

A handwritten signature in cursive script that reads "Matt Ludwig". The signature is written in black ink and is positioned above a horizontal line.

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](http://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](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, North Carolina, or Rhode Island**, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)
- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

**If you are a resident of Rhode Island**, note that pursuant to Rhode Island 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.

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.