17283

Key Food Updates Customers on Payment Card Data Incident

MATAWAN, NEW JERSEY – JULY 16, 2020 – Key Food Stores Co-Operative, Inc. ("Key Food") values the relationship it has with its customers and takes the security of payment card data very seriously. Key Food is providing additional information about the payment card incident that was first reported on March 2, 2020. Key Food conducted an investigation of the incident with its Co-Op members, notified the payment card networks and followed their investigation process, and continues to provide information to assist an investigation by law enforcement.

The investigation identified the installation of malware designed to access payment card data from cards used on point-of-sale ("POS") devices at one Co-Op Member store located in Massachusetts between April 7, 2019 and January 24, 2020. The POS devices at the store location involved were EMV (chip) enabled. For EMV transactions at this location, Key Food believes that only the card number and expiration date would have been found by the malware (but not the cardholder name or internal verification code). For transactions where the magnetic stripe on the back of the card was swiped at the POS device, the malware could have found track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code). There is no indication that other customer information was affected.

Customers can access a list of the locations involved and specific timeframes, as well information about additional steps they can take at *www.keyfood.com/store/protectingourcustomers*. Not all locations were involved, and the specific timeframes vary by location.

During the investigation, Key Food removed the malware and implemented enhanced security measures. Key Food also continues to look for additional steps to enhance the security of payment card data. In addition, Key Food is working with the payment card networks so that the banks that issued the payment cards involved can be made aware.

Consistent with good practices, customers should closely monitor their payment card statements for any unauthorized activity. Unauthorized transactions should immediately be reported to the bank that issued the card 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 typically on the back of your payment card.

If customers have questions regarding this incident, they can visit the website above or call 1-855-907-2134. Monday through Friday between the hours of 9:00 a.m. and 9:00 p.m. ET.

###

Media Contact:
Rachel Hemsworth
Public Relations
rgeissler@keyfood.com

Notice of Payment Card Data Incident

July 16, 2020

Key Food Updates Customers on Payment Card Data Incident

Key Food is providing additional information about the payment card incident that we first reported on March 2, 2020. Key Food conducted an investigation of the incident with our Co-Op Members. We notified the payment card networks, followed their investigation process, and continue to provide information to assist the investigation by law enforcement.

The investigation identified the installation of malware designed to access payment card data from cards used on point-of-sale ("POS") devices at some but not all Co-Op Member stores. The POS devices at the store locations involved were EMV enabled. For EMV transactions at these locations, we believe only the card number and expiration date would have been found by the malware (but not the cardholder name or internal verification code). For transactions where the magnetic stripe on the back of the card was swiped at the POS device, the malware could have found track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code). The malware was not present on all POS devices at every involved location, and the timeframes when malware was present are different across the locations involved.

A list of all locations involved and specific timeframes can be accessed below.

During the investigation, Key Food removed the malware and implemented enhanced security measures. Key Food will also continue to look for additional steps to enhance the security of payment card data. In addition, Key Food has been working with the payment card networks so that the banks that issued the payment cards involved can be made aware.

Consistent with good practices, customers should closely monitor their payment card statements for any unauthorized activity. Unauthorized transactions should immediately be reported to the bank that issued the card 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 typically on the back of your payment card. More information on identity theft prevention is available *below*.

If you have additional questions, you can call 1-855-907-2134, Monday through Friday between the hours of 9:00 a.m. and 9:00 p.m. ET.

Additional Steps You Can Take

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 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, 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 and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Massachusetts: Under 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, as described above. 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

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

Select where your payment card was used

STATE

Select a state