BakerHostetler

Baker&Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

October 20, 2017

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)
AND OVERNIGHT MAIL

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, Whole Foods Market Services, Inc. (WFM), to notify you of a security incident involving Washington residents.

On September 23, 2017, WFM learned of unauthorized access of payment card information used at certain venues such as tap rooms and full table-service restaurants located within some stores. These venues use a different point of sale system than WFM's primary store checkout systems, and payment cards used at the primary store checkout systems were not affected. When WFM learned of potential unauthorized access, WFM launched an investigation, obtained the help of a leading cyber security forensics firm, and contacted law enforcement. WFM replaced these point of sale systems for payment card transactions and stopped the unauthorized activity.

The investigation determined that unauthorized software was present on the point of sale system at certain venues. The software copied payment card information—which could have included payment card account number, card expiration date, internal verification code, and cardholder name—of customers who used a payment card at these venues at dates that vary by venue but are no earlier than March 10, 2017 and no later than September 28, 2017.

WFM does not collect the mailing or email address from customers when they use their payment card at WFM venues. Thus, WFM is not able to identify the names and mailing

addresses of all individuals that used their card at the affected venues during the specific time frames. Additionally, although WFM knows the affected venue locations, not all payment cards used at these venues were affected. Accordingly, WFM is unable to identify the number of Washington residents that used a card at an identified venue. Instead, on October 20, 2017, pursuant to Wash. Rev. Code § 19.255.010(8)(c), WFM provided substitute notification by posting a statement on its website (www.wholefoodsmarket.com/customernotification), providing a link to the statement on its homepage, and issuing a press release (a copy of the press release and substitute notice are enclosed). Notice is being provided as expeditiously as practicable and without unreasonable delay.

WFM has established a dedicated call center that potentially affected individuals can contact with questions. WFM is also recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

WFM has worked closely with the payment card networks as well as with the cyber security forensics firm to stop the unauthorized activity and evaluate ways to enhance security measures.

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

Sincerely,

Theodore J. Kobus III
Partner

Enclosures

Whole Foods Market Payment Card Investigation Update

October 20, 2017 01:23 PM Eastern Daylight Time

AUSTIN, Texas--(BUSINESS WIRE)--Whole Foods Market (Nasdaq: WFM) has resolved the incident previously announced on September 28, 2017, involving unauthorized access of payment card information used at certain venues such as tap rooms and full table-service restaurants located within some stores. These venues use a different point of sale system than the company's primary store checkout systems, and payment cards used at the primary store checkout systems were not affected. Whole Foods Market learned of the unauthorized access on September 23, 2017. The company conducted an investigation, obtained the help of a leading cyber security forensics firm, and contacted law enforcement. Whole Foods Market replaced these point of sale systems for payment card transactions and stopped the unauthorized activity. Whole Foods Market apologizes to customers for any inconvenience or concern this may have caused.

The investigation determined that unauthorized software was present on the point of sale system at certain venues. The software copied payment card information—which could have included payment card account number, card expiration date, internal verification code, and cardholder name—of customers who used a payment card at these venues at dates that vary by venue but are no earlier than March 10, 2017 and no later than September 28, 2017.

The Amazon.com systems do not connect to these systems at Whole Foods Market. Transactions on Amazon.com have not been impacted.

Whole Foods Market has been working closely with the payment card companies. Payment card network rules generally state that cardholders are not responsible for fraudulent charges that are reported in a timely manner. Customers should promptly report any unauthorized charges to the bank that issued their card. The phone number to call is usually on the back of the payment card.

For additional information, including additional steps you may take to protect yourself, please visit www.wholefoodsmarket.com/customernotification. This site also contains a list of the venues involved, although not all cards used at all venues listed were affected.

If you have any questions, please call 1-888-818-7100 from 8:00 a.m. to 5:00 p.m. C.T., seven days a week.

Contacts

Whole Foods Market
Brooke Buchanan, 512-279-0231
media@wholefoods.com

Whole Foods Market Payment Card Investigation Update

California residents please click here.

AUSTIN, Texas (October 20, 2017) – Whole Foods Market has resolved the incident previously announced on September 28, 2017, involving unauthorized access of payment card information used at certain venues such as tap rooms and full table-service restaurants located within some stores. These venues use a different point of sale system than the company's primary store checkout systems, and payment cards used at the primary store checkout systems were not affected. Whole Foods Market learned of the unauthorized access on September 23, 2017. The company conducted an investigation, obtained the help of a leading cyber security forensics firm, and contacted law enforcement. Whole Foods Market replaced these point of sale systems for payment card transactions and stopped the unauthorized activity. Whole Foods Market apologizes to customers for any inconvenience or concern this may have caused.

The investigation determined that unauthorized software was present on the point of sale system at certain venues. The software copied payment card information—which could have included payment card account number, card expiration date, internal verification code, and cardholder name—of customers who used a payment card at these venues at dates that vary by venue but are no earlier than March 10, 2017 and no later than September 28, 2017.

The Amazon.com systems do not connect to these systems at Whole Foods Market. Transactions on Amazon.com have not been impacted.

Whole Foods Market has been working closely with the payment card companies. Payment card network rules generally state that cardholders are not responsible for fraudulent charges that are reported in a timely manner. Customers should promptly report any unauthorized charges to the bank that issued their card. The phone number to call is usually on the back of the payment card.

Please see the section that follows this notice for additional steps you may take to protect yourself. The drop-down form below contains a list of the venues involved, although not all cards used at all venues listed were affected.

If you have any questions, please call 1-888-818-7100 from 8:00 a.m. to 5:00 p.m. C.T., seven days a week.

[DROP DOWN LIST:]

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain 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:

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
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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

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

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
(410) 576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-877-566-7226

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.

- Each of the nationwide credit reporting companies – Experian, TransUnion, and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- 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. And 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 may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Whole Foods Market Payment Card Investigation Update

NOTICE OF DATA BREACH

AUSTIN, Texas (October 20, 2017) – Whole Foods Market has resolved the incident previously announced on September 28, 2017, involving unauthorized access of payment card information used at certain venues such as tap rooms and full table-service restaurants located within some stores. Whole Foods Market apologizes to customers for any inconvenience or concern this may have caused.

What Happened

Whole Foods Market learned on September 23, 2017 of unauthorized access of payment card information used at certain venues such as taprooms and full table-service restaurants located within some stores. These venues use a different point of sale system than the company's primary store checkout systems, and payment cards used at the primary store checkout systems were not affected.

What Information Was Involved

The investigation determined that unauthorized software was present on the point of sale system at certain venues. The software copied payment card information—which could have included payment card account number, card expiration date, internal verification code, and cardholder name—of customers who used a payment card at these venues at dates that vary by venue but are no earlier than March 10, 2017 and no later than September 28, 2017. The Amazon.com systems do not connect to these systems at Whole Foods Market. Transactions on Amazon.com have not been impacted.

What You Can Do

Whole Foods Market has been working closely with the payment card companies. Payment card network rules generally state that cardholders are not responsible for fraudulent charges that are reported in a timely manner. Customers should promptly report any unauthorized charges to the bank that issued their card. The phone number to call is usually on the back of the payment card. Please see the section that follows this notice for additional steps you may take to protect yourself. The drop-down form included at **www.wholefoodsmarket.com/customernotification** contains a list of the venues involved, although not all cards used at all venues listed were affected.

What We Are Doing

When Whole Foods Market learned of potential unauthorized access, it conducted an investigation, obtained the help of a leading cyber security forensics firm, and contacted law

enforcement. Whole Foods Market replaced these point of sale systems for payment card transactions and stopped the unauthorized activity.

For More Information

If you have any questions, please call 1-888-818-7100 from 8:00 a.m. to 5:00 p.m. C.T., seven days a week.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain 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:

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
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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