Moe's California Substitute Notice

[Will appear on: www.moes.com/paymentcardnotification]

October 2, 2019

NOTICE OF DATA BREACH

Moe's Southwest Grill values the relationship we have with our customers and understands the importance of protecting payment card information. We initially notified our customers on August 20, 2019 that we were investigating a payment card security incident involving some of our corporate and franchised restaurants. We immediately began an investigation, took action to identify and stop the unauthorized activity, and forensic investigation firms were engaged. We also notified law enforcement and the payment card networks.

What Happened?

A thorough investigation is being conducted and is nearly complete. It appears that unauthorized code designed to copy payment card data from cards used in person was installed in certain corporate and franchised restaurants at different times over the general period of April 29, 2019 to July 22, 2019. The unauthorized code was not present at all locations, and at most locations it was present for only a few weeks in July. A list of the Moe's Southwest Grill locations involved and the respective time frames, which vary by location, is available *here*.

At two locations, separate, unrelated, but similar incidents were identified during the investigation. The time frames for those two locations (one in Hawaii and the other in New Jersey) can be found in the list referenced above.

What Information Was Involved?

The unauthorized code searched for track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. The code often found the part of track data that contains the card number, expiration date, and internal verification code, and sometimes it found the part that also includes the cardholder name. It is possible the code did not find every card that had been used at each location during the time frames involved.

What We Are Doing.

We quickly took measures to contain the incident, remove the unauthorized code, and we are working to implement measures to further enhance payment card security.

What You Can Do.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your 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 usually

on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any questions, please call (877) 269-5073 from 9:00 a.m. to 7:00 p.m. ET, Monday through Friday.

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 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

McAlister's California Substitute Notice

[Will appear on: www.mcalistersdeli.com/paymentcardnotification]

October 2, 2019

NOTICE OF DATA BREACH

McAlister's Deli values the relationship we have with our customers and understands the importance of protecting payment card information. We initially notified our customers on August 20, 2019 that we were investigating a payment card security incident involving some of our corporate and franchised restaurants. We immediately began an investigation, took action to identify and stop the unauthorized activity, and forensic investigation firms were engaged. We also notified law enforcement and the payment card networks.

What Happened?

A thorough investigation is being conducted and is nearly complete. It appears that unauthorized code designed to copy payment card data from cards used in person was installed in certain corporate and franchised restaurants at different times over the general period of April 29, 2019 to July 22, 2019. The unauthorized code was not present at all locations, and at most locations it was present for only a few weeks in July. A list of the McAlister's Deli locations involved and the respective time frames, which vary by location, is available *here*.

What Information Was Involved?

The unauthorized code searched for track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. The code often found the part of track data that contains the card number, expiration date, and internal verification code, and sometimes it found the part that also includes the cardholder name. It is possible the code did not find every card that had been used at each location during the time frames involved.

What We Are Doing.

We quickly took measures to contain the incident, remove the unauthorized code, and we are working to implement measures to further enhance payment card security.

What You Can Do.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your 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 usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any questions, please call (877) 269-5073 from 9:00 a.m. to 7:00 p.m. ET, Monday through Friday.

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 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

Schlotzsky's California Substitute Notice

[Will appear on: www.schlotzskys.com/paymentcardnotification]

October 2, 2019

NOTICE OF DATA BREACH

Schlotzsky's values the relationship we have with our customers and understands the importance of protecting payment card information. We initially notified our customers on August 20, 2019 that we were investigating a payment card security incident involving some of our corporate and franchised restaurants. We immediately began an investigation, took action to identify and stop the unauthorized activity, and forensic investigation firms were engaged. We also notified law enforcement and the payment card networks.

What Happened

A thorough investigation is being conducted and is nearly complete. It appears that unauthorized code designed to copy payment card data from cards used in person was installed in certain corporate and franchised restaurants at different times over the general period of April 11, 2019 to July 22, 2019. The unauthorized code was not present at all locations, and at most locations it was present for only a few weeks in July. A list of the Schlotzsky's locations involved and the respective time frames, which vary by location, is available *here*.

At one location in Kansas, a separate, unrelated, but similar incident was identified during the investigation. The time frame for that location can be found in the list referenced above.

What Information Was Involved.

The unauthorized code searched for track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. The code often found the part of track data that contains the card number, expiration date, and internal verification code, and sometimes it found the part that also includes the cardholder name. It is possible the code did not find every card that had been used at each location during the time frames involved.

What We Are Doing.

We quickly took measures to contain the incident, remove the unauthorized code, and we are working to implement measures to further enhance payment card security.

What You Can Do.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your 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 usually

on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

For More Information

We regret that this occurred and apologize for any inconvenience. If you have any questions, please call (877) 269-5073 from 9:00 a.m. to 7:00 p.m. ET, Monday through Friday.

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 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