SpencerFane®

Shawn Tuma
Direct Dial: 972-324-0317
stuma@spencerfane.com

File No. 5033115-0001

November 26, 2019

VIA CERTIFIED MAIL

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

Re: Notification of Data Incident

Dear Sir/Madam:

We are providing this Notification of Data Incident on behalf of our client, On The Border (the "Company"). The Company's corporate office is located at 2201 West Royal Lane, Ste 240, Irving, Texas 75063.

The Company is actively investigating a security incident that involves a payment processing system that services some of its restaurants. On November 14, 2019, the Company determined that some of its guests' payment card information was accessed through malware installed on a payment processing system. The Company learned that the security incident may have involved payment cards processed between April 10, 2019, through August 10, 2019 at certain On The Border restaurants in the following states: Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, and Virginia. Not all On The Border restaurants have been impacted by this incident.

The Company has already taken steps to contain and remediate the incident. Upon learning of this incident, the Company immediately began working to identify and remove the malware which led to the compromise. The company has retained a leading forensics firm and is conducting an investigation to determine the extent to which information in the Company's systems have been impacted. The Company is cooperating with law enforcement and have also notified the payment card networks of the investigation.

The Company believes the security incident impacted only payment card information, which includes names, credit card numbers, credit card expiration dates, and credit card verification codes. The Company does not collect social security numbers, full dates of birth, or identification numbers of its guests. Therefore, these identifiers were not compromised.

Because the Company does not collect contact information of its guests at the time payment card transactions are executed, the Company is unable to confirm the number of affected residents in your state (or whether any residents of your state are actually affected). For the same reason, the Company is unable to directly notify the potentially affected individuals. Therefore, as of November 26, 2019, the Company has provided notification of this incident on its website, along with a set of Frequently Asked Questions addressing this incident. The Company has also distributed a press release to media outlets in your state.

Copies of the website notice, Frequently Asked Questions, and the press release are attached. The Company has also established a call center to address additional questions potentially affected individuals may have. Additionally, because the Company cannot determine which transactions were executed by distinct guests, the Company is unable to determine an accurate number of total individuals affected by this incident.

The Company maintains a written information security program and the Company is in the process of determining whether updates to the plan are appropriate as a result of this incident.

The Company is committed to protecting the privacy and security of the data of its guests. Be assured that the Company will continue to exercise vigilance and use what they have learned from this incident to further strengthen their safeguards. As the Company's investigation progresses, we will inform your office of any significant developments concerning this incident should they arise.

Please let me know if you have any questions about the information provided in this notice.

Respectfully yours,

Shawn E. Tuma

Enclosures:
Website Notice
Frequently Asked Questions
Press Release

ON THE BORDER

PRESS RELEASE

For Immediate Distribution

Notice of Potential Payment Card Incident

DALLAS (Nov. 26, 2019) – On The Border is actively investigating a security incident that involves a payment processing system servicing some of our restaurants. On November 14, 2019, we determined that some of our guests' payment card information was accessed through malware installed on a payment processing system.

Our company has retained a leading forensics firm and is conducting an investigation to determine the extent to which information in On The Border's system has been impacted. We are cooperating with law enforcement and have also notified payment card networks of the investigation.

We learned that the security incident may have involved payment cards processed at certain restaurants between April 10, 2019, through August 10, 2019. Not all On The Border restaurants have been impacted by this incident. Additionally, this incident does not affect guests who made purchases for catering orders, nor does it affect our franchisees. We have already taken steps to contain and remediate the incident. We have determined this incident involves certain On The Border restaurants in the following states: Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, and Virginia.

To ensure guests have the latest information, we have set up a dedicated page on our website – https://www.ontheborder.com/security. Guests may call our call center at 833-918-2053, which is open between 8 a.m. and 8 p.m. CST Monday through Friday (excluding federal holidays).

On The Border is committed to protecting the privacy and security of our guests and will continue to take quick action. While our investigation continues, we remind all of our guests to be vigilant and that it is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

Contact: Call Center at 833-918-2053.

###

NOTICE OF POTENTIAL PAYMENT CARD INCIDENT

What Happened?

On The Border is actively investigating a security incident that involves a payment processing system that services some of our restaurants. On November 14, 2019, we determined that some of our guests' payment card information was accessed through malware installed on a payment processing system.

Our company has retained a leading forensics firm and is currently investigating the extent to which information in On The Border's system has been impacted. We are cooperating with law enforcement and have also notified payment card networks of the investigation.

We have learned that the security incident may have involved payment cards processed at certain restaurants between April 10, 2019, through August 10, 2019. Not all On The Border restaurants have been impacted by this incident. Additionally, this incident does not affect guests who have made purchases for catering orders, nor does it affect our franchisees. We have already taken steps to contain and remediate the incident. We have determined this incident involves certain On The Border restaurants in the following states: Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, and Virginia.

To ensure guests have the latest information, we have set up a dedicated page on our website – https://www.ontheborder.com/security (https://www.ontheborder.com/security). Guests may call our call center at 833-918-2053, which is open between 8 a.m. and 8 p.m. CST Monday through Friday (excluding federal holidays).

On The Border is committed to protecting the privacy and security of our guests and will continue to take quick action. While our investigation continues, we remind all of our guests to be vigilant and that it is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

When Did This Happen?

We believe that payment cards used at certain restaurants between April 10, 2019, through August 10, 2019, may have been impacted.

What Information Was Involved?

We believe the security incident impacted only payment card information which could include names, credit card numbers, credit card expiration dates, and credit card verification codes. We do not collect social security numbers, full dates of birth, or identification numbers of guests. Therefore, those identifiers were not compromised.

What We Are Doing.

On The Border values the privacy and the trust placed in us by our guests. We regularly update and strengthen our systems and processes to help prevent unauthorized access. Upon learning of this incident, we immediately began remediating the issue by working to identify and remove the malware which led to the potential compromise. As part of our ongoing commitment to protecting guest information and privacy, we are working with leading partners in cybersecurity to strengthen and enhance the security of our systems as we go forward.

Our investigation into this incident is ongoing. We will continue to exercise vigilance and use what we have learned from this incident to strengthen our safeguards. We have notified the payment card networks and law enforcement of this incident and we are cooperating with each of their investigations.

For More Information.

We have set up a dedicated page on our website – https://www.ontheborder.com/security (https://www.ontheborder.com/security) – where we will post information and any updates about this incident.

What You Can Do.

Your use of a payment card at On The Border restaurants in the states identified between April 10, 2019, through August 10, 2019, does not automatically mean that your information was compromised. However, we encourage our guests to stay vigilant, to continually review credit and debit card statements for irregular or unauthorized charges, and to immediately report any unauthorized charges to your financial institution.

Additionally, we recommend you take one or more of the following actions to help protect your information:

1. Review your credit reports, and debit and credit card statements. We recommend that you regularly review account statements and monitor credit reports. Frequently review all banking statements for purchases, withdrawals, checks, or other activity not authorized by you. You should continually monitor your accounts even if you do not initially notice issues. Criminals may hold information for extended periods of time before using it.

Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com (www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting

1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com
(www.alerts.equifax.com)	(www.experian.com)	(www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact one of the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them, at https://www.identitytheft.gov/ (https://www.identitytheft.gov/).

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy (http://www.ca.gov/Privacy)) for additional information on protection against identity theft. ().

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov (www.ag.ky.gov), Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer (www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf (www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov (www.ncdoj.gov), Telephone: 1-919-716-6400

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/ (www.doj.state.or.us/), Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov (www.riag.ri.gov), Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft (www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

FREQUENTLY ASKED QUESTIONS

What Happened?

On The Border is actively investigating a security incident that involves a payment processing system that services some of its restaurants. On November 14, 2019, On The Border determined that some of its guests' payment card information was accessed through malware installed on a payment processing system. On The Border's investigation revealed that the security incident may have involved payment cards processed at certain restaurants between April 10, 2019, through August 10, 2019.

Not all On The Border restaurants have been impacted by this incident. Additionally, this incident does not affect guests who have made purchases for catering orders, nor does it affect On The Border franchisees.

On The Border has already taken steps to contain and remediate the incident. On The Border has determined this incident involves certain On The Border restaurants in the following states: Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, and Virginia.

When did this happen?

On The Border believes that payment cards used at certain restaurants between April 10, 2019, through August 10, 2019, may have been impacted.

What personal information was involved?

On The Border believes the security incident may have impacted only payment card information which could include names, credit card numbers, credit card expiration dates, and credit card verification codes.

On The Border does not collect social security numbers, full dates of birth, or identification numbers of guests. Therefore, those identifiers were not compromised.

What locations are involved?

On The Border's investigation of this incident is ongoing. The locations affected by this incident include certain On The Border restaurants in the following states: Arkansas, Arizona, Colorado, Connecticut, Florida, Georgia, Iowa, Illinois, Indiana, Kansas, Massachusetts, Maryland, Maine, Michigan, Missouri, Mississippi, North Carolina, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, and Virginia. On The Border will update this website to reflect any changes to this list based on its ongoing investigation if necessary.

Does this incident affect On The Border guests who ordered using food delivery apps such as Door Dash, Uber Eats, Grubhub, or Postmates?

No. On The Border's investigation revealed that the security incident was limited to payment cards processed at certain restaurants between April 10, 2019, through August 10, 2019. Food delivery apps

process On The Border orders through their own payment processing systems. Payment information is not transmitted to On The Border during such transactions.

Has law enforcement been notified?
On The Border has notified law enforcement of this incident and is cooperating with their investigation.

If there are any updates regarding this incident, how will I be notified?
If additional updates are provided, that information will be posted at https://www.ontheborder.com/security (https://www.ontheborder.com/security).

Who should I contact if I have questions?
Guests may call our call center at 833-918-2053, which is open between 8 a.m. and 8 p.m. CST Monday through Friday (excluding federal holidays).
