

Appendix B

NOTICE OF DATA BREACH

Updated May 18, 2018

Available at <https://www.jasonsdeli.com/data-breach>

What Happened?

On December 22, 2017, Jason's Deli was notified by payment processors that credit card security personnel had informed it that a large quantity of payment card information had appeared for sale on the "dark web," and that an analysis of the data indicated that at least a portion of the data may have come from various Jason's Deli locations. Jason's Deli's management immediately activated our response plan, including engagement of a leading threat response team, involvement of other forensic experts, and cooperation with law enforcement. We first released a preliminary public statement on December 28, 2017 describing our initial response, and later on January 11, 2018 posted this Notice of Data Breach capturing findings in the early stages of our investigation.

After completing a thorough forensic investigation, we confirm that criminals deployed RAM-scraping malware on a number of our point-of-sales (POS) terminals at various corporate-owned Jason's Deli restaurants (see below for a list) starting on June 8, 2017. During the course of our investigation, our response team contained the breach and disabled the malware in all of the locations where it was discovered.

What Information Was Involved?

We believe that the criminals used the malware to obtain payment card information off of the POS terminals beginning on June 8, 2017 and ending on December 29, 2017. Our investigation has determined that approximately 3.4 million unique payment cards were used on the impacted POS terminals during this period. Specifically, the payment card information obtained was full track data from a payment card's magnetic stripe. While this information varies from card issuer to card issuer, full track data can include the following: cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code. However, it should be noted that the cardholder verification value that may have been compromised is not the same as the security code printed on the back of certain payment cards (e.g., Discover, MasterCard, and Visa) or printed on the front of other payment cards (e.g., American Express). In addition, the track data does not include personal identification numbers ("PINs") associated with debit cards.

We previously reported on January 11, 2018 that approximately 2 million unique payment cards may have been exposed, and we want to explain the difference in volume between that earlier estimate and what we now believe to be a more accurate number. Unlike a situation in which a

Deli Management, Inc.
Updated Notice of a Data Breach

block of static data is illegally copied and stolen all at once, the RAM-scraping malware employed by the criminals against Jason's Deli copied data as individual transactions occurred on the affected POS terminals over a specific period of time. Our preliminary count was based on the transaction data we had available to us at the time. We recently obtained from our payment processor the complete set of transactions that may have been impacted. Using that more complete information, we now believe the number to be approximately 3.4 million cards.

What Are We Doing?

Since the breach was discovered and throughout the entire investigative process, Jason's Deli has worked closely with third-party forensics and cyber security firms, as well as federal law enforcement, to investigate and contain the breach. In addition, we are working to make whatever changes may be necessary to strengthen our systems against attack, and are investing in advanced network monitoring capabilities and improving our payment systems to protect the security of your information.

What Can You Do?

The security of your information is important to us, and we are working hard to ensure that it is protected. There are also things you can do:

First, to determine whether you may have been affected by this security breach, we recommend that you review the list of impacted Jason's Deli restaurants (**see below for a list**) and review your credit and debit card statements for any unauthorized charges. If you think you have been affected, please contact (i) your credit or debit card company to report the potential unauthorized activity; and (ii) contact us at customer.service@jasonsdeli.com or call 409-838-1976 (Monday through Friday, 8am to 5pm CT), to obtain more information about the breach and the options available to you at this time.

Furthermore, we encourage our customers to remain vigilant by reviewing your credit and debit account statements, as well as your credit report, 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 agencies, listed below. To obtain your annual free credit report, please visit www.annualcreditreport.com or call 1-877-322-8228.

Equifax	Experian	TransUnion
P.O. Box 740256 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 105281 Atlanta, GA 30348 1-888-909-8872 www.transunion.com

Other Important Information:

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 consumer protection 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. Moreover, you should obtain a copy of the police report in the event your creditors request a copy to correct your records.

Federal Trade Commission: Contact information for the Federal Trade Commission is as follows: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.ftc.gov/idtheft, or call 1-877-IDTHEFT (438-4338).

For California Residents: You may contact the California Attorney General's Office at California Department of Justice, Attn: Office of Privacy Protection, P.O. Box 944255, Sacramento, CA 94244, or call 916-322-3360. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.oag.ca.gov.

For Iowa Residents: You may contact the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, or call 515-281-5164. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.iowaattorneygeneral.gov.

For Maryland Residents: You may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, or call 1-888-743-0023. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.oag.state.md.us.

For Massachusetts and Rhode Island Residents:

- Under Massachusetts and Rhode Island laws, you have the right to obtain a copy of any police report.
- Security Freeze: Massachusetts and Rhode Island laws also allow consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be mindful that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.
- The fee for placing a security freeze on a credit report is \$5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.
- To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Deli Management, Inc.
Updated Notice of a Data Breach

- **Equifax Security Freeze**, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com, or call 1-800-685-1111.
- **Experian Security Freeze**, P.O. Box 9554, Allen, TX 75013, www.experian.com, or call 1-888-397-3742
- **TransUnion Security Freeze**, P.O. Box 2000, Chester, PA 19022, www.transunion.com, or call 1-888-909-8872.
- In order to request a security freeze, you will need to provide the following information:
 - Your full name (including middle initial as well as Jr., Sr., II, III, etc.),
 - Social Security number,
 - Date of birth,
 - If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years,
 - Proof of current address such as a current utility bill or telephone bill,
 - A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.), and
 - 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 three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.
- To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For New Mexico Residents: New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

- You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

Deli Management, Inc.
Updated Notice of a Data Breach

- The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.
- The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:
 1. the unique personal identification number, password or similar device provided by the consumer reporting agency;
 2. proper identification to verify your identity;
 3. information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
 4. payment of a fee, if applicable.
- A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.
- A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.
- If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For North Carolina Residents: You may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, or call 919-716-6400. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.ncdoj.gov.

For Oregon Residents: You may contact the Oregon Attorney General's Office at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301, or call 1-877-877-9392. You can

Deli Management, Inc.
Updated Notice of a Data Breach

also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.doj.state.or.us.

For West Virginia Residents:

- 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. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is provided above.
- As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit <http://www.ftc.gov/idtheft>.
- You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.
- The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique PIN or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:
 1. The unique PIN or password provided by the consumer reporting agency;
 2. Proper identification to verify your identity; and
 3. The period of time for which the report shall be available to users of the credit report.
- A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.
- A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.
- If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. We advise that you plan

Deli Management, Inc.
Updated Notice of a Data Breach

ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, several days before actually applying for new credit.

For More Information:

Please contact Jason's Deli at 350 Pine Street, Suite 1775, Beaumont, TX 77701, email customer.service@jasonsdeli.com, or call 409-838-1976, Monday through Friday, 8am to 5pm CT.