BARNES & THORNBURG LLP

11 S. Meridian Street
Indianapolis, IN 46204-3535 U.S.A.
(317) 236-1313
Fax (317) 231-7433

www.btlaw.com

Brian J. McGinnis
Attorney
(317) 231-6437
Brian.Mcginnis@btlaw.com

October 2, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Security Event Notice Provided for Grant Street Inn

Dear Attorney General MacDonald:

Barnes & Thornburg LLP acts as attorneys for the Grant Street Inn ("Grant Street"), an entity incorporated in the State of Indiana and located at 310 North Grant Street, Bloomington, Indiana, 47408, with respect to a data security event involving Sark Technologies LLC, d/b/a SuperINN ("SuperINN") and the exposure of certain personal information as described in more detail below.

1. Nature of the Security Event

SuperINN was recently the victim of a cybersecurity attack that resulted in a data breach. SuperINN is a third party online reservation and guest management vendor. SuperINN notified Grant Street Inn that SuperINN was the victim of a cybersecurity attack that resulted in a data breach, which SuperINN believes may have exposed the names and payment information of guests of Grant Street Inn. SuperINN maintained the relevant personal information on SuperINN servers and Grant Street Inn's systems have not been affected by this breach.

2. Number of New Hampshire Residents Affected

Two (2) of the affected individuals are residents of New Hampshire and the information related to these individuals included the name, credit card information, home and credit card billing addresses, telephone number, and email address. Although the information disclosed was encrypted, SuperINN believes that the attacker also obtained the decryption keys, which most likely permitted the attacker to decrypt the stolen information.

3. Steps Taken or Planned to be Taken Related to the Security Event

Upon learning of the breach from SuperINN, Grant Street Inn took immediate action to contact and work with SuperINN to identify Grant Street Inn guests that may have had their personal information subjected to unauthorized access as a result of the SuperINN breach and to

identify the respective individuals' contact information to be able to provide affected individuals notification of the breach.

SuperINN has since informed Grant Street Inn that SuperINN is ceasing all operations. Grant Street Inn is in the process of identifying a new reservation system service provider. As part of its incident response, Grant Street Inn is reviewing its data protection and privacy practices and policies and will be performing a privacy assessment as part of its due diligence to engage with an alternate service provider.

As outlined in the attached breach notification letter, Grant Street has provided the affected individuals with the information related to their rights to place a security freeze on a credit report and to place a fraud alert.

4. Contact Information

Please contact the undersigned with any questions regarding this incident.

Very truly yours,

BARNES & THORNBURG LLP

Brian J. McGinnis

cc: Cynthia Kretz, Grant Street Inn

September [xxxDatexxx], 2019

%first_name% %last_name%

%guests_address%
%guests_city_name%, %guests_state_name% %guests_zipcode%

%guest_email%

NOTICE OF DATA BREACH

PLEASE READ THIS ENTIRE NOTIFICATION

Dear %first_name% %last_name%:

We are contacting you regarding a data security breach that may have impacted your personal information. Sark Technologies LLC, d/b/a SuperINN ("SuperINN") provides online reservation and guest management services to hotels and inns. SuperINN recently notified our inn, the Grant Street Inn in Bloomington, Indiana, that SuperINN was recently the victim of a cybersecurity attack that resulted in a data breach. SuperINN believes their breach may have exposed the names and payment information of guests of Grant Street Inn. SuperINN maintained the relevant personal information on SuperINN servers and Grant Street Inn's systems have not been affected by this breach.

What Happened? On August 4, 2019, SuperINN advised Grant Street Inn that SuperINN became aware of a security breach of SuperINN's systems on May 26, 2019. Since SuperINN's notification, we have been working with SuperINN to determine what happened and which of our guests may have been affected.

Due to the nature of the breach, SuperINN and its technology forensics provider were not able to confirm any actual access to or attempted misuse of your information. We are contacting you because your information may have been exposed as a result of this cybersecurity incident. Please note that at this time we have no indication that any fraud to our guests has resulted from the SuperINN breach.

What Information Was Involved? We are providing you with this notice as SuperINN's breach may have involved unauthorized access to and disclosure of your personal information, including your: name, credit card information, home and credit card billing addresses, telephone number, and email address.

What We Are Doing? SuperINN has investigated the breach to assess any potential harm to you and has taken steps necessary to address and mitigate the incident. Grant Street Inn is committed to protecting your information and is taking steps to address this incident and the protection of our guests' information with our vendor.

SuperINN has provided the following technical summary of the incident and their subsequent investigation:

- One or more attackers identified a vulnerability in an image upload function of the SuperINN Plus web application available to authenticated users that allowed the attacker to upload PHP web shells. The earliest of these web shells found on the system was dated September 23, 2018.
- Correlated with these web shells, the investigation identified PHP scripts used to export data from the SuperINN Plus database, including encrypted card numbers. It is assumed that the attacker had also obtained the decryption key using a PHP web shell. The earliest evidence of exported data available included records dated January 1, 2019 and later. The export of data continued through May 30, 2019. Sark Technologies became aware of the incident on May 26, 2019.
- By June 3, 2019, Sark Technologies had (a) identified and removed the PHP web shells and (b) reconfigured the web application to prevent the ability to upload PHP files.
- In addition to the PHP web shell, an attacker identified a SQL injection vulnerability in the web application and appeared to make use of it to pull encrypted cardholder data from the database. Available logs showed this SQL injection being used in June and July 2019. It is again assumed that the attacker had previously obtained the decryption key using a PHP web shell. By July 16, 2019, Sark Technologies had (a) identified and removed the SQL injection vulnerability and (b) rotated encryption keys.
- Based on this information, the window of potential exposure for card data has been set as September 23, 2018, through July 16, 2019.

What Is Being Done To Protect Your Information? SuperINN has advised us that they are working diligently to ensure that all of its systems, processes and practices related to guests' credit card and personal information are reviewed and improved in an effort to prevent such incidents in the future. SuperINN has engaged a third party to conduct a forensic investigation, which has resulted in the correction of the underlying issue. Furthermore, SuperINN's systems are undergoing "penetration testing," which is designed to identify any other vulnerabilities in the systems. If any further vulnerabilities are discovered, those will be corrected as well.

What you can do to protect your information? Additional actions you can consider taking to reduce the chances of identity theft or fraud on your accounts are provided within this letter.

Our Contact Information. We understand that you may have questions about this incident that are not addressed in this letter. We are happy to address these questions as we are able and invite you to contact %NAME%, %TITLE% at Grant Street Inn at %PHONE% or %EMAIL% for further information.

Finally, on behalf of Grant Street Inn, please allow us to sincerely apologize for any inconvenience this incident may cause.

Sincerely,
Grant Street Inn
(assumed business name of CFC, LLC)

ADDITIONAL ACTIONS TO HELP REDUCE CHANCES OF IDENTITY THEFT

We have included below the contact information for the three nationwide credit reporting agencies. As a precautionary measure, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company which maintains the account. You also should promptly report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint about identity theft with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services/

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit

reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

    - Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

    - The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Federal Trade Commission
Visit the FTC website at www.ftc.gov
Call 1-877-ID-THEFT or
Write to:
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

California Residents:
The data security incident may have involved unauthorized access to and disclosure of your personal information, including: name, credit card information, home and credit card billing addresses, telephone number, and email address.

For Illinois Residents:
The Federal Trade Commission can be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261, www.identitytheft.gov.

Maryland Residents:
Contact the Maryland Attorney General's Identity Theft Unit:
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
410-576-6566 idtheft@oag.state.md.us

Massachusetts Residents:

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer credit report without written authorization. However, please be aware 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.

If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. If you provide the credit reporting agency with a copy of the police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services/

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

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 personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

In order to lift the security freeze 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 identities 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.

North Carolina
Visit the North Carolina Office of the Attorney General at http://www.ncdoj.gov/Crime.aspx
Call 1-919-716-6400 or
Write to:
Attorney General's Office
9001 Mail Service Center

Oregon Residents
It is also advisable to report suspected incidents of identity theft to Federal Trade Commission or the Oregon Attorney General at https://www.doj.state.or.us/consumer-protection/