



15499

Risto Pribisich  
200 Public Square, Suite 2300  
Cleveland, Ohio 44114-2378  
Phone: (216) 363-4686  
Fax: (216) 363-4588  
rpribisich@beneschlaw.com

***VIA ONLINE SUBMISSION***

August 2, 2019

Office of Consumer Affairs and Business Regulation  
501 Boylston St.  
Suite 5100  
Boston, MA 02116

***RE: Notice of Data Security Incident***

To Whom it May Concern,

We are contacting you on behalf of our client, Sark Technologies LLC ("SuperINN.com"), of Cleveland Heights, Ohio, regarding a recent data security incident at the company. SuperINN.com's investigation determined that the data security incident affected approximately 43,250 individuals residing across the U.S. and in 64 other countries, including 2,166 residents of Massachusetts.

Our client is in the process of notifying its customers and the affected individuals. A template of the letter being sent to affected Massachusetts residents on behalf of SuperINN.com's customers is attached to this Notice for your review.

Below is a summary of the incident and 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, names, home and credit card billing addresses, telephone numbers, and email addresses of SuperINN.com's customers' guests. 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 exported data continued through May 30, 2019. SuperINN.com became aware of the incident May 26, 2019.

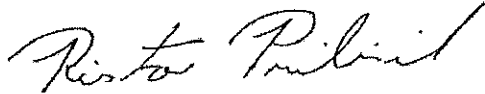
By June 3, 2019 SuperINN.com had (a) identified and removed the PHP web shells and (b) reconfigured the web application to prevent the ability to upload PHP files.

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, SuperINN.com 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.

SuperINN.com sincerely regrets this data security incident and any inconvenience it may cause the affected individuals. Should you have any questions or concerns regarding this matter, please do not hesitate to contact me at 216-363-4686 or [rpribisich@beneschlaw.com](mailto:rpribisich@beneschlaw.com).

Sincerely,

A handwritten signature in cursive script that reads "Risto Pribisich".

Risto Pribisich  
BENESCH, FRIEDLANDER,  
COPLAN & ARONOFF LLP

Property Generic Letterhead

[Date], 2019

[Insert Recipient's Name]  
[Insert Address]  
[Insert City, State, Zip]  
[Insert Recipient's Email Address]

***RE: Important Data Security and Protection Notification***

**PLEASE READ THIS ENTIRE NOTIFICATION**

Dear [Name]:

We are contacting you regarding a data security incident that occurred at our online guest management and reservation system provider ("Vendor"). The data security incident, which is more fully described below, occurred in May 2019. Our Vendor became aware of the incident on May 26, 2019, and provided notice of the incident to us on [date], 2019. 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.

Our Vendor has investigated the incident to assess any potential harm to you and is taking steps necessary to address and mitigate the incident. Both [Property Name] and our Vendor are committed to protecting all the information that you have entrusted to us.

The following is a summary of the incident and 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

I, 2019 and later. The exported data continued through May 30, 2019. Our Vendor became aware of the incident May 26, 2019.

By June 3, 2019 our Vendor 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, our Vendor 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.

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's 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: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze Fraud & Identity Theft P.O. 2000 Chester, PA 19016
---	--	--

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.

#### **What is being done to protect your information:**

In light of this incident, our Vendor is 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. Since the incident, our Vendor has engaged a third party to conduct a forensic investigation, which has resulted in the correction of the underlying issue. Furthermore, our Vendor'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:**

You should remain vigilant by reviewing your account statements and monitoring your credit reports. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the final page of this letter.

We sincerely regret this data security incident and any inconvenience it may cause you and encourage you to take advantage of the identity theft protection offered by our Vendor. Should you have any questions or concerns regarding this matter, please do not hesitate to contact [Name of Contact at Property] by phone at [(XXX) XXX-XXXX] or email at [Email Address].

Sincerely,

[Name]

[Title]

[Property Name]

## **ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT**

### **➤ 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.

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
Information Services	Consumer Assistance Center	P.O. Box 1000
P.O. Box 105065	P.O. Box 4500	Chester, PA 19022
Atlanta, GA 30348-5069	Allen, TX 75013	1-800-680-7289
1-800-525-6285	1-888-397-3742	<a href="http://www.transunion.com">www.transunion.com</a>
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	

### **➤ 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.

### **➤ ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit [www.annualcreditreport.com](http://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](http://www.ftc.gov/idtheft). The address for the FTC is:

Federal Trade Commission  
Attn: CRC-240  
600 Pennsylvania Avenue, NW  
Washington, D.C. 20580