



Mark A. Mattingly

P 314.552.6122

F 314.552.7122

mmattingly@thompsoncoburn.com

December 24, 2015

James Boffetti  
Bureau Chief, Consumer Protection and Antitrust  
c/o Mary Thayer, Secretary  
Mary.thayer@doj.nh.gov

Re: Data Breach Potentially Affecting Personal Information of One New Hampshire Resident

Dear Mr. Boffetti:

On behalf of our client, SAS Safety Corporation (the “Company”), we write to advise you of an incident involving the unauthorized introduction of malware onto the Company’s website, [www.sassafety.com](http://www.sassafety.com). This malware resulted in the possible compromise of personal information of a Company customer residing in New Hampshire. Based upon the Company’s investigation, the malware was present from September 23, 2015 to December 8, 2015 and potentially exposed certain personal information of one resident that was inputted by that customer. The personal information that was potentially affected by the incident includes: customer name, address, credit or debit card number, payment card expiration date and the card’s CVV security number. Additionally, the customer’s logon identification and password for the website may have been affected. The Company does not collect customers’ social security or driver’s license numbers and that data was in no way affected by the incident.

The Company has no knowledge that any of the potentially affected customers’ personal information has been misused as a consequence of this incident, including but not limited, to any instance of identity theft.

The Company discovered the incident on December 7, 2015 after receiving reports that the website was exhibiting unusual behavior. The Company immediately investigated the reports. The Company’s investigation determined that malware affecting its Magento ecommerce software had been inserted on September 23, 2015. The malware potentially caused the data described above to be copied as it was inputted by the customer. The malware was eliminated on December 8, 2015 by corrective action taken by the Company. The Company continues to closely monitor for any recurrence of the malware.

Since learning of the incident, the Company has taken important measures to improve the level of its data security including the following: adding developers to improve data security, consulting with developers outside the Company to improve data security with the Magento ecommerce software used by the Company, installing additional patches, modifying admin passwords and closely monitoring the website for this, and other, threats. These measures are designed to reduce the risk of a recurrence of the malware and strengthen the Company’s overall posture against unauthorized access of personal information. The Company takes data security seriously and has not suffered any other incidents requiring notice to its customers.

Thompson Coburn LLP | Attorneys at Law | One US Bank Plaza | St. Louis, Missouri 63101

P 314.552.6000 | F 314.552.7000 | [www.thompsoncoburn.com](http://www.thompsoncoburn.com)

Chicago • Los Angeles • St. Louis • Southern Illinois • Washington, D.C.

In addition to technical measures, the Company has taken several other steps in response to the incident. The Company reported the incident to law enforcement. Additionally, the Company retained outside counsel to provide advice as to the Company's legal obligations potentially arising from the incident. The Company is also committed to notifying all of its potentially affected customers.

To enable the potentially affected customers to take steps in response to the incident, the Company will promptly notify each such customer of the incident by sending notices via first-class mail on December 24, 2015. A copy of the notice is enclosed with this letter. In addition to describing the incident, the notice provides information regarding protective measures that may be taken in response as well as a toll free number for customers to call with any questions.

We trust that this letter and its enclosure provide you with all of the information required to assess this incident and the Company's response. Please let us know if you have any questions or if we may be of further assistance. You may contact the undersigned with any inquiries.

Very truly yours,

Thompson Coburn LLP



By  
Mark A. Mattingly

MAM/law

Encl.



 **ADDRESS**  
3031 Gardenia Avenue  
Long Beach, CA 90807

 **TOLL FREE & FAX**  
1 (800) 262-0200  
1 (800) 244-1938

 **WEB**  
info@sassafety.com  
www.sassafety.com

December 24, 2015

Dear [Name],

Protecting customer privacy and personal information is a top concern of SAS. You are receiving this notice because we recently learned of a security incident that potentially affected personal information of customers who made payment card purchases on our website, [www.sassafety.com](http://www.sassafety.com), between September 23, 2015 and December 8, 2015. We are providing this notice to inform potentially affected customers of the incident and to call their attention to some steps they can take in response to this incident. We sincerely apologize for any inconvenience or concern this incident may cause you.

We began investigating the incident immediately upon learning of it. Based upon our investigation, it appears the incident occurred when harmful computer code, known as "malware," was inserted without our knowledge or permission onto our website. This malware may have accessed customer information as it was input by customers during the checkout process. The information potentially affected by this incident includes customer name and address, credit or debit card number, and the payment card's expiration date and "CVV" security number. Your online account ID and password may have also been affected. No payment card pin numbers were affected. No social security numbers, driver's license numbers or other government identification numbers are requested during the checkout process and those numbers were NOT affected.

We acted immediately once the incident was discovered to determine the scope of the unauthorized access and we took measures to remove the malware. We continue to monitor for this malware and other risks as part of our ongoing efforts to protect your personal information. Additionally, we added security measures that are designed to further bolster our data security and to help prevent incidents of this kind in the future.

Although we are unaware of any instances of fraud or identity theft arising from this incident, we want to make potentially affected customers aware of steps they can take to guard against fraud or identity theft. You should change your online account password at our website. You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institution by contacting the number on the back of the payment card. As a general rule, customers are not liable for fraudulent transactions, but again, you should regularly and carefully review your account statements. You may also contact your financial institution and request a new payment card.



You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

**Equifax**

(800) 525-6285  
P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)

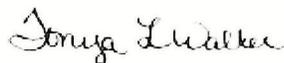
**Experian**

(888) 397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

**TransUnion**

(800) 680-7289  
Fraud Victim Assistance Division  
P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)

The privacy and protection of our customers' personal information is a matter we take very seriously. If you have any questions or concerns, please do not hesitate to contact us at 800-262-0200 or write to us at 3031 Gardenia Avenue, Long Beach, California 90807. Again, we want to stress that we regret any inconvenience or concern caused by this incident.



Marketing Manager  
SAS Safety Corp.