



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

April 20, 2020

VIA EMAIL

Attorney General Tom Miller
Office of the Attorney General
Consumer Protection Division
Security Breach Notifications
1305 E Walnut Street
Des Moines, IA 50319-0106
Email: consumer@ag.iowa.gov

Re: Notice of Data Security Incident

Dear Attorney General Miller:

We represent Volusion, LLC (“Volusion”), an e-commerce platform that hosts websites for online merchants, with regard to a recent data security incident described in greater detail below. This letter is being sent on behalf of Volusion because personal information belonging to Iowa residents may have been affected by a recent data security incident.

1. Nature of the security incident.

On or about October 8, 2019, Volusion learned that personal information of some customers of Volusion’s merchant clients may have been improperly exposed as a result of malware placed on Volusion’s e-commerce platform. Immediately after learning this, Volusion took steps to secure their platform, removed the malware, notified the FBI, began an investigation and hired independent cybersecurity experts to assist with that investigation. On March 20, 2020, following a thorough independent investigation, Volusion confirmed that personal information input by some customers of Volusion’s merchant clients may have been improperly exposed while making purchases on the merchant clients’ websites between September 7, 2019 and October 8, 2019.

The information may have included names, addresses, phone numbers, email addresses, credit card numbers, CVVs, and expiration dates.

2. Number of Iowa residents affected.

Approximately 4,020 residents of Iowa were affected by this incident. Volusion will be notifying the potentially affected Iowa residents on or about April 20, 2020. A sample copy of the notification communication is being provided with this correspondence. In addition, Volusion is notifying statewide media and posting notice of the incident on their website.

3. Steps taken relating to the incident.

In addition to the steps discussed above, Volusion updated its internal procedures based on the findings of the investigation and added additional safeguards to minimize the chance that an incident like this could occur in the future.

4. Contact information.

Volusion remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at lindsay.nickle@lewisbrisbois.com.


Please let me know if you have any questions.

Very truly yours,

A handwritten signature in cursive script, appearing to read "L. Nickle".

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter.

 Volusion <do-not-reply@volusion.idexperts-notification.info>
To:

^Account.DATE(LONG)

Dear First Name,

Re: Notice of Data Incident

We are writing to inform you of a data security incident that may have involved your personal information. At Volusion, we take the privacy and security of personal information very seriously and apologize for any inconvenience this incident may have caused you. This notice includes information about steps you can take to protect yourself and your personal information.

What Happened?

Volusion is an e-commerce platform that hosts websites for many online merchants. On or about October 8, 2019, we learned that personal information of some customers of our merchant clients may have been improperly exposed as a result of malware placed on Volusion's e-commerce platform. Immediately after learning this, Volusion took steps to secure the platform, removed the malware, notified the FBI, began an investigation, and hired independent cybersecurity experts to assist with that investigation. On March 20, 2020, following a thorough independent investigation, we confirmed that personal information input by some customers of our merchant clients may have been improperly exposed while making purchases on our merchant clients' websites between September 7, 2019 and October 8, 2019. Your information may have been impacted.

What Information Was Involved?

Based on our investigation, the affected personal information may have included names, addresses, phone numbers, email addresses, credit card numbers, CVVs, and expiration dates. According to our records, the card number associated with your name ended in <<insert variable text of last 4 digits>>.

What Are We Doing?

In addition to the steps discussed above, Volusion updated its internal procedures based on the findings of the investigation and added additional safeguards to minimize the chance that an incident like this could occur in the future.

What You Can Do.

We encourage you to review and follow the recommendations included with this notice. In addition, we recommend that you carefully review your payment card account statements, and if you find any suspicious activity report it to the financial institution that issued the account. You can also report any suspected fraudulent activity to local law enforcement.

For More Information.

If you have any questions, please call 1-833-968-1686, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. You may also visit <https://ide.myidcare.com/volusion> for more information.

Sincerely,

Lance Wright

Lance Wright

Chief Information Security Officer

Volusion, LLC

Steps you can Take to Further Protect your Information

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion	Free Annual Report
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 12 months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including the Attorney General in your state.

Federal Trade Commission	Rhode Island	Maryland Attorney General	North Carolina Attorney General
600 Pennsylvania Ave, NW	Attorney General	200 St. Paul Place	9001 Mail Service Center
Washington, DC 20580	150 South Main Street	Baltimore, MD 21202	Raleigh, NC 27699
consumer.ftc.gov , and	Providence, RI 02903	oag.state.md.us	ncdoj.gov
www.ftc.gov/idtheft	http://www.riag.ri.gov	1-888-743-0023	1-877-566-7226
1-877-438-4338	401-274-4400		

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.