staminus
4695 MacArthur Court, 11th Floor
Newport Beach, CA 92660

Via UPS and Email

April 11, 2016

Joseph A. Foster, Attorney General
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

I am writing to inform you that on March 10, 2016, Staminus Communications ("Staminus") was the victim of an unauthorized intrusion into its network. As a result of this intrusion, systems were temporarily taken offline and customer information was exposed. On March 11, Staminus posted a preliminary notice of the incident on its website, and subsequently emailed active customers to inform them of the incident.

The protection of the personal information of its customers is very important to Staminus. Upon discovering this intrusion, Staminus took immediate action, including launching an investigation, notifying law enforcement, restoring its systems, and putting additional security measures into place to help prevent a future incident. For example, we have relaunched our billing platform, partnering with leading payment processors, Stripe and Zuora. We have also implemented multi-factor authentication requirements. In addition, we continue to work with the FBI in its investigation of the incident.

Staminus' investigation into the incident is ongoing. Staminus has determined that the personal information (as defined in N.H. Rev. Stat. § 359-C:19(III)) of residents of New Hampshire was affected by the incident. Based on our investigation to date, we know that name and credit card number, as well as usernames, passwords, and contact information, was exposed. As of now, Staminus believes that the personal information of 12 New Hampshire residents was affected. We are in the process of notifying individuals whose personal information was affected, and plan to mail notice letters to New Hampshire residents on or around April 15, 2016. Enclosed is a sample copy of the notice that will be sent to New Hampshire residents.

If you have any questions or require additional information, please feel free to contact me at 949.202.5305 x2101, or matt.mahvi@staminus.net.

Sincerely,

Matt Mahvi
CEO
Staminus Communications

Encl.

staminus
4695 MacArthur Court, 11th Floor
Newport Beach, CA 92660

Dear Customer:

We are writing this letter to inform you of a data security incident that involved some of your personal information.

What Happened?

On March 10, 2016, Staminus Communications was the victim of an unauthorized intrusion into its network. As a result of this intrusion, systems were temporarily taken offline and customer information was exposed. The protection of the personal information of its customers is very important to Staminus. Upon discovering this attack, Staminus took immediate action, including launching an investigation into the attack, notifying law enforcement, restoring its systems, and putting additional security measures into place to help prevent a future incident.

What Information Was Involved?

Based on our initial investigation, we know that names and credit card numbers, as well as usernames, passwords, and contact information, were exposed. Staminus' investigation into the incident is ongoing.

What Are We Doing?

In addition to the steps noted above (e.g., restoring our systems and notifying law enforcement), we have relaunched our billing platform, partnering with leading payment processors, Stripe and Zuora. We have also implemented multi-factor authentication requirements. We also are continuing to work with the Federal Bureau of Investigation ("FBI") in its investigation of the incident. We continue to work with law enforcement in their investigation of this breach, and our notice to you has not been delayed as a result of any law enforcement investigation.

In addition, we have taken steps to notify credit card companies of the credit card numbers that may have been accessed during this incident. Your credit card company may contact you to verify charges if it detects any unusual pattern of activity, or to replace your credit card. While we have taken steps to notify your credit card company proactively, we recommend that you also immediately notify your credit card issuing bank and follow its advice with regard to your credit card.

What You Can Do

- ***Contact Your Credit Card Issuer.*** As noted, we have taken steps to notify credit card companies of the credit card numbers impacted. Even so, you should remain vigilant by carefully reviewing your credit card account statements and immediately alerting your credit card issuing bank of any suspicious charges. This is the most important step that you can take to detect and prevent any unauthorized use of your credit card number.

- ***Change Your Passwords.*** While the Staminus passwords compromised were hashed, it is possible that the decryption key was compromised as well. Thus, you should immediately change your Staminus password. Additionally, we highly recommend customers who utilize similar credentials across different platforms reset any passwords on accounts that may use the same or a similar password to their Staminus login.

- ***Be Aware of Phishing Schemes.*** You should also always be on the lookout for phishing schemes. Any email correspondence we may send regarding this matter will not contain a link, so if you receive an email appearing to be from us that contains a link, it is not from us, and you should not click on the link. Also, never provide sensitive information to unsolicited requests

staminus
4695 MacArthur Court, 11th Floor
Newport Beach, CA 92660

claiming to come from us, your bank or other organizations. We would never ask you for sensitive information via email.

- ***Regularly Review Your Financial Statements.*** We recommend you remain vigilant by regularly reviewing your credit card and bank account statements.

- ***Obtain a Free Credit Report.*** You may request a free copy of your U.S. credit report once every 12 months by visiting www.annualcreditreport.com or by calling 1-877-322-8228 toll free. You can print a copy of the request form at http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm.

- ***Carefully Review Your Credit Report.*** Look for accounts you did not open and inquiries from creditors that you did not initiate. Also, look for personal information, such as your home address, that is inaccurate. If you see anything that is wrong or that you do not understand, call the credit reporting agency at the telephone number on the report. We also suggest that you consider contacting one of the major credit bureaus listed below to place a fraud alert or security freeze on your credit reports:

	Equifax	Experian	TransUnion
Phone	1-800-525-6285 or 1-888-766-0008	1-888-397-3742	1-800-680-7289
Address	Equifax Consumer Fraud Division PO Box 740256 Atlanta, GA 30374	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	https://www.experian.com/consumer/cac/InvalidateSession.do?code=SECURITYALERT	http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page

- ***Place a Security Freeze on Your Account.*** In addition to a fraud alert, you may also have a security freeze placed on your credit file. A security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to $10.00 to place a freeze or lift or remove a freeze. To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online.

	Equifax	Experian	TransUnion
Address	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp	https://www.experian.com/freeze/center.html	https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

- ***Contact Law Enforcement.*** If you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-

438-4338), or write to Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580 for additional guidance.

Other Important Information

- ***Federal Trade Commission.*** The Federal Trade Commission also provides helpful information about fraud alerts, security freezes, and how to avoid identity theft.
- ***State-Specific Information.*** If you are a resident of one the following states, the following information applies to you.
  - **For residents of Maryland, North Carolina, and Rhode Island:** For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
Phone	1-410-576-6491	1-877-566-7226 (within North Carolina) or 1-919-716-6000 (if outside North Carolina)	1-401-274-4400
Email	Idtheft@oag.state.md.us	consumer@ncdoj.gov	consumers@riag.ri.gov
Address	Identity Theft Unit Attorney General of Maryland 200 St. Paul Place 16th Floor Baltimore, MD 21202	Consumer Protection Division Attorney General's Office Mail Service Center 9001 Raleigh, NC 27699-9001	Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903
Website	https://www.oag.state.md.us/	http://www.ncdoj.gov	http://www.riag.ri.gov/

  - **For residents of Rhode Island:** Under Rhode Island law, you have the right to obtain a police report filed 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.

For More Information

We sincerely regret that this happened and will continue to put the right measures in place to maintain the security of your information. Should you have any questions or other concerns about this matter, please don't hesitate to contact us at:

- **Email**: matt.mahvi@staminus.net
- **Phone**: [INSERT]
- **Address**: 4695 MacArthur Court, 11th Floor
  Newport Beach, CA 92660

Sincerely,

Matt Mahvi

staminus™
4695 MacArthur Court, 11th Floor
Newport Beach, CA 92660

CEO
Staminus Communications