



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED
NOV 19 2018

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 13, 2018

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

Dear Attorney General MacDonald:

We represent StataCorp LLC (“StataCorp”), 4905 Lakeway Drive, College Station, Texas 77845, and are writing to notify you of a recent incident that may affect the security of the personal information of four (4) New Hampshire residents. By providing this notice, StataCorp does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

Nature of the Data Event

On September 18, 2018, StataCorp discovered a JavaScript code was placed in the footer of its shopping cart by an unauthorized individual. StataCorp immediately removed the code and launched an investigation to determine the nature and scope of the incident. StataCorp’s investigation determined the code was placed in the shopping cart on September 13, 2018 and remained until StataCorp’s removal on September 18, 2018. The code permitted an unauthorized individual access to certain StataCorp customer information including name, phone number, address, account username and password, and credit card information.

StataCorp took immediate steps to confirm the security of its systems, reset passwords, and provided preliminary notice of the incident via email to all impacted customers on September 21, 2018.

Notice to New Hampshire Residents

The potentially impacted individuals were provided notice via email to their email address on file with StataCorp on September 21, 2018. A copy of the notice email is attached hereto as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the unauthorized access to customer payment card information, StataCorp moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident. StataCorp is also working to implement additional safeguards to protect the security of information in its system, including continuous monitoring for system updates and conducting scans for malicious activity.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at 267-930-4786.

Very truly yours,

A handwritten signature in blue ink that reads "Ryan Loughlin".

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/mb
Enclosure

EXHIBIT A

Subject: Security notification from StataCorp
From: "Stata" <service@stata.com>
Date: 9/21/2018 3:40 PM
To: [REDACTED]

A security incident affecting the StataCorp website may have impacted you.



Dear [REDACTED],

We are writing to inform you about a security incident affecting the StataCorp website that we believe may have impacted you.

What happened?

On Tuesday, September 18, we discovered that Javascript code had been placed in the footer of our shopping cart by an unauthorized third party via the administrative login page. We immediately removed the unauthorized code.

By Wednesday, September 19, we learned through our investigation that the code was placed in the shopping cart on Thursday, September 13, and that while it was active, it could cause the web browser of anyone who submitted a form in the shopping cart to send the same data to an unauthorized third party. These data could include contact information such as name, phone number, and address and could also include credit card information if that was submitted.

Who was affected?

A small portion (about 1,700 users) of our customer base accessed our shopping cart during this time period. We are notifying all potentially affected customers along with any relevant regulatory and privacy agencies. You are being notified because our records show that you submitted an order or interacted with our shopping cart during the incident time period.

StataCorp's internal databases were not compromised. This incident consisted of a client-side scripting exploit that may have resulted in data being sent directly from your web browser to the unauthorized third party.

What has StataCorp done?

The unauthorized code has been removed from the server, and we continue to carry out scans to ensure that the server remains clean. We have changed administrative passwords and have restricted administrative access to the server.

We apologize that this happened and will take all appropriate steps to ensure the integrity and security of our shopping cart. We take our obligations under privacy and information security laws seriously. We have engaged a number of third-party advisors to ensure that we deal with this incident promptly and thoroughly and that we comply with all applicable legal and regulatory requirements.

We already implement regularly scheduled scans of our website and shopping cart software to ensure security and compliance with the Payment Card Industry Data Security Standard (PCI DSS). We have now implemented additional automated scans of our website and shopping cart software to protect against such an exploit in the future.

What should I consider doing?

While we have not been notified of any adverse impact to our customers at this point, we advise that you monitor your credit card usage to ensure that charges after the date range above were only made by you. You should notify your credit card issuer of the incident and any account activity you do not recognize.

If you have a StataCorp shopping cart username and password, we have randomized your password to protect against unauthorized access to your account. You will be required to reset your password before accessing your shopping cart account in the future. If you use the same combination of username and password with any other websites, we recommend that you also change these credentials.

To protect against phishing attacks, you should carefully review emails purporting to be from StataCorp to verify the origin address and domain before clicking on any link or file or providing any information. Never provide online credentials to unsolicited requests claiming to come from us or other institutions. Additionally, you can learn more about phishing and how to recognize it here:

<https://www.consumer.ftc.gov/articles/0003-phishing>

Next steps

We believe we fully understand the extent of this exploit, but our investigation remains ongoing, and we will contact you again in due course if there are any relevant updates. If you have any immediate questions, please contact us at service@stata.com.

Sincerely,

[REDACTED]

service@stata.com | 1-979-696-4600
© 2018 StataCorp LLC. All rights reserved.
4905 Lakeway Drive, College Station, TX 77845, USA



— Attachments: —

image001.gif

0 bytes