mwe.com

Laura Jehl
Attorney at Law
ljehl@mwe.com
+1 202 756 8930

July 27, 2020

VIA EMAIL / SECURITYBREACH@ATG.WA.GOV
Office of the Attorney General
Attorney General Bob Ferguson
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504

Re: BrainGenie – Security Incident Notification

Dear Attorney General Ferguson:

We represent CK-12 Foundation (CK-12) with respect to a data security incident involving potential exposure of certain personal information described in detail below. CK-12 is a non-profit foundation that operates the BrainGenie website, a free online resource of educational materials. CK-12 cares about the security of its website users' personal information and has taken steps to prevent a similar event from occurring in the future.

1. **Nature of the incident**

In early June, CK-12 became aware of a report that mentioned Braingenie as one of a number of websites impacted by a potential security incident. CK-12 promptly commenced an investigation, with the assistance of outside forensic experts and law enforcement, to assess whether the incident affected any of Braingenie's user information.

The investigation determined that beginning sometime in late February, CK-12's systems were accessed without authorization. On July 15, CK-12 was able to determine that unauthorized actors obtained a small amount of personal information from a Braingenie test (QA) database. Since discovering this, CK-12 has continued to assess what personal information was impacted and to identify affected individuals.

Based on reports and our investigation, CK-12 believes the personal information that may have been affected includes user login credentials for Braingenie accounts, which for some users includes username and/or email address and password. Although CK-12 protects its users' passwords using encryption, CK-12 believes that unauthorized actors may have later been able to derive text passwords for some accounts.

2. **Steps taken in response to the incident**

After learning of this incident, CK-12 has reviewed its security protocols and has taken additional steps to enhance its security. CK-12 has also directed users to change their passwords, including prompting users to do so when they try to log into their account.

CK-12 has been in communication with law enforcement and are continuing to cooperate with their wider investigation.

3. Number of residents impacted

CK-12 has identified 5,017 Washington residents who were potentially impacted by this incident. Electronic notification will be sent to each of these individuals between July 28, 2020 and August 10, 2020. We enclose a copy of the form notification letter.

4. Contact information

Please contact me at ljehl@mwe.com or (202) 756-8930 if you have any questions.

Sincerely,

Laura Jehl

Enclosures

Notice of Data Security Incident

Note: Only a subset of Braingenie users were impacted by this security incident.

What happened?

In early June, we became aware of a report that mentioned Braingenie as one of a number of websites impacted by a potential security incident. We promptly commenced an investigation, with the assistance of outside forensic experts and law enforcement, to assess whether the incident affected any of Braingenie's user information.

The investigation determined that beginning sometime in late February, our systems were accessed without authorization. On July 15, we were able to determine that unauthorized actors obtained a small amount of personal information from a Braingenie test (QA) database. Since discovering this, we have continued to assess what personal information was impacted and to identify affected individuals.

What information was involved?

Based on reports and our investigation, we believe the personal information that may have been affected includes user login credentials for Braingenie accounts, which for some users includes username and/or email address and password. Although we protect our users' passwords using encryption, we believe that unauthorized actors may have later been able to derive text passwords for some accounts.

What are we doing?

After learning of this incident, we have reviewed our security protocols and have taken additional steps to enhance our security.

We have been in communication with law enforcement and are continuing to cooperate with their wider investigation.

What you can do.

We recommend that you change your password for your Braingenie account. The next time you login to Braingenie, you will be prompted to change your password. Please choose a strong password that is not easy to guess and is not one that you use for any other online account.

We also recommend that you change your password for any other online accounts for which you use the same username and password, or email address and password, combination.

Please contact us if you notice any suspicious activity in your Braingenie account.

More information.

If you have any questions about this incident or about resetting your BrainGenie password, you may contact us at support@braingenie.com or +1 (650) 272-0606.

Though we do not collect or maintain your financial information, we are required by law to notify you of the following:

We recommend that you remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe you are a victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission (FTC) and/or the Office of the Attorney General (AGO) in your state. You may also report any suspected identity theft to law enforcement.

For more information about steps you can take to avoid identity theft, including information about fraud alerts and security freezes, you can contact the FTC, your AGO, or any of the major credit reporting agencies.

For your convenience, here is the contact information for the FTC:

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Here is the contact information for the three major credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

For New York residents, you may contact and obtain information from these state agencies:

New York Office of the Attorney General	New York Department of State	New York Division of State Policy
www.ag.ny.gov	www.dos.ny.gov	www.ny.gov/agencies/division-state-police
(800) 771-7755	800-697-1220	(914) 834-9111