EXHIBIT 1

We represent Animoto Inc. ("Animoto") located at 333 Kearny Street 6th Floor, San Francisco, CA 94108, and are writing to notify your office of an incident that may affect the security of some personal information relating to 8,842 Delaware residents. By providing this notice, Animoto does not waive any rights or defenses regarding the applicability of Delaware law, the applicability of the Delaware data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 6, 2018, Animoto confirmed that suspicious activity on its system may have resulted in the unauthorized acquisition of user data, including dates of birth, geolocation, hashed and salted passwords, and usernames (user email addresses). While the passwords were salted and hashed (a process that obscures the password), it is unknown whether the salt key was acquired.

Animoto first learned of suspicious activity on July 10, 2018, when it received an alert of unusual activity on its system. Upon review, Animoto identified queries being run against its user database. Animoto immediately stopped the queries and launched an investigation with the assistance of third-party experts. On August 6, 2018, Animoto's investigation confirmed the queries were unauthorized and that user data may have been obtained on or around July 10, 2018. While Animoto cannot confirm that data was removed from its systems or that any particular user information was affected, Animoto is advising its users about this incident out of an abundance of caution. The information that was accessed may have included first name, last name, username (email address), hashed and salted passwords, geolocation, gender, and date of birth. Complete payment card data is stored in a separate system that was not accessed.

Notice to Delaware Residents

On or about August 16, 2018, Animoto began providing rolling notice of this incident to all potentially impacted individuals. Animoto does not keep address information for most users, and does not have geolocation information for all users. Animoto has approximately 985 users whose addresses are located in Delaware, and 7,857 users who geolocate to Delaware. Please note geolocation information does not mean Animoto can confirm state of residency. Notice is being provided by email in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Animoto moved quickly to investigate and respond to the incident, assess the security of Animoto systems, and notify potentially affected individuals. Animoto is also working to implement additional safeguards. Animoto changed employee passwords and is urging all users to change their passwords immediately. In addition to working with experts to conduct an investigation, Animoto replaced system passwords and reduced the number of users who could access certain systems. Animoto continues to monitor for suspicious activity and make enhancements with their systems to detect and prevent unauthorized access to user information including rebuilding infrastructure to make it more secure. Further, Animoto is examining ways to enhance overall network cyber threat detection technology and has reported this incident to law enforcement.

EXHIBIT A

Notice of Data Breach

Dear Animoto Community,

I'm writing to notify you about an issue that may involve your Animoto account information. We value your privacy and, therefore, we want to provide you with details about the event, what data was involved, and the steps we're taking to protect your information.

What Happened? On July 10, 2018, we received an alert of unusual activity on our system. We immediately stopped all suspicious activity and launched an investigation with the support of outside forensics experts. On August 6, 2018, we confirmed that the activity was unauthorized, and that user data may have been obtained. **While we cannot confirm that data was removed from our systems or that your information was affected, we wanted to let you know about this incident out of an abundance of caution.**

What Information Was Involved? We determined that, as a result of the activity, data was accessed on July 10, 2018. The data may have included first name, last name, username (your email address), hashed and salted passwords, geolocation, gender, and date of birth. While the passwords were hashed and salted (a method used to secure passwords with a key), it's unclear whether or not the key was accessed. Complete payment card data was stored in a separate system and was not accessed. To date, Animoto has no evidence of any actual or attempted fraudulent misuse of information as a result of this incident.

What We Are Doing. We take this event, and the security of your information, very seriously. We are reviewing our policies and procedures to better protect against an event like this happening again in the future. In addition to working with third-party experts to