Exhibit 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Atlanta Botanical Garden does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, Atlanta Botanical Garden received notification from Blackbaud of a cyber incident on its network. Blackbaud is a cloud computing provider that provides financial services tools to non-profit organizations, including Atlanta Botanical Garden. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud reported that the threat actor was able to exfiltrate data from Blackbaud's network at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 2020 that Blackbaud notified Atlanta Botanical Garden that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified Atlanta Botanical Garden of this incident, it reported that certain information, such as tax identification number, was encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor.

On September 29, 2020, Blackbaud notified Atlanta Botanical Garden that, contrary, to its previous representations, certain tax identification numbers may have been subject to unauthorized access or acquisition. Blackbaud reported that these tax identification numbers had been transferred into an unencrypted state without Atlanta Botanical Garden's knowledge, and this information may have been accessible to the threat actor. Atlanta Botanical Garden immediately investigated this expanded scope to confirm the individuals to whom this information related and worked with Blackbaud to determine the list of individuals whose unencrypted tax identification numbers were present on Blackbaud's network at the time of the incident. On or about October 16, 2020, Blackbaud provided the updated information on these records, at which time Atlanta Botanical Garden reviewed and identified one (1) Maine resident whose name, address, and tax identification number may have been subject to unauthorized acquisition.

Notice to Maine Resident

On November 13, 2020, Atlanta Botanical Garden began providing written notice of the Blackbaud incident to one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of this event, Atlanta Botanical Garden moved quickly to investigate and to respond to the incident, including notifying potentially affected individuals. Atlanta Botanical Garden is reviewing its procedures with third-party vendors, including Blackbaud. Atlanta Botanical Garden is providing access to credit monitoring services for 24 months to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Atlanta Botanical Garden is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Atlanta Botanical Garden is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Exhibit A

ATLANTA BOTANICAL GARDEN

Atlanta | Gainesville

November 13, 2020

[Name]
[Address Line 1]
[City] [State] [Zip Code]

Dear [Name]:

Atlanta Botanical Garden ("ABG") writes to inform you of a recent incident involving one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), that may have affected the privacy of some of your information. *While we have no evidence of any actual or attempted misuse of any information as a result of this incident*, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On July 16, 2020, ABG received notification from Blackbaud of a cyber incident on its network. Blackbaud is a cloud computing provider that provides financial services tools to non-profit organizations, including ABG. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud reported that the threat actor was able to exfiltrate data from Blackbaud's network at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 2020 that Blackbaud notified ABG that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified ABG of this incident, it reported that certain information, such as Tax identification numbers, was encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor.

On September 29, 2020, Blackbaud notified ABG that, contrary, to its previous representations, certain tax identification numbers may have been subject to unauthorized access or acquisition. Blackbaud reported that these Tax identification numbers had been transferred into an unencrypted state without ABG's knowledge, and this information may have been accessible to the threat actor. ABG immediately investigated this expanded scope to confirm the individuals to whom this information related and worked with Blackbaud to determine the list of individuals whose unencrypted tax identification numbers were present on Blackbaud's network at the time of the incident. On or about October 16, 2020, Blackbaud provided us with updated information on these records. We then worked internally to confirm the individuals affected and provide notification of this incident.

What Information Was Involved? Our investigation determined that the potentially impacted personal information included your name and taxpayer identification number. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by an unknown actor.

What Are We Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing procedures regarding our third-party vendors. ABG is continuing to work with Blackbaud to address relevant questions and the next steps that Blackbaud is taking to remediate its data privacy event. Please note that Blackbaud confirmed it will be removing this historical unencrypted ABG information from its network. We will also be notifying state regulators, as required.

Although ABG is unaware of any actual or attempted misuse of your information as a result of this incident, Blackbaud offering you access to credit monitoring services for 24 months at no cost to you as an added precaution. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

1345 PIEDMONT AVENUE NE
ATLANTA, GEORGIA 30309
404-876-5859 | FAX 404-8767472

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information and a description of services and instructions on how to enroll in these services.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at 855-914-4704 9:00 am to 9:00 pm Eastern Time, Monday through Friday (excluding some U.S. national holidays) starting on Wednesday, November 18, 2020. You may also write to Atlanta Botanical Garden at 1345 Piedmont Avenue, Atlanta, GA 30309.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

ATLANTA BOTANICAL GARDEN

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

We are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

To enroll in Credit Monitoring services, please visit: **https://www.cyberscouthq.com/epiq263?ac=263HQ1517**. If prompted, please provide the following unique code to gain access to services: **263HQ1113**.

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. This notice has not been delayed by law enforcement.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If

you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.