

# **EXHIBIT 1**

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Delaware Nature Society 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 Thursday, July 16, 2020, Delaware Nature Society received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Delaware Nature Society. Upon receiving notice of the cyber incident, Delaware Nature Society immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Delaware Nature Society data.

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 investigate. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Delaware Nature Society immediately began to determine what, if any, sensitive Delaware Nature Society data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident.

The information that could have been subject to unauthorized access for the potentially affected Delaware residents includes individual’s name, health insurance information, and allergy information.

### **Notice to Delaware Resident**

On August 31, 2020, Delaware Nature Society provided written notice of this incident to all affected individuals, which includes six hundred twenty-four (624) Delaware residents. 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 discovering the event, Delaware Nature Society moved quickly to investigate and respond to the incident, review our existing policies and procedures regarding our third-party vendors, and work with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, Delaware Nature Society 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. Delaware Nature Society is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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**



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
 <<address\_1>>  
 <<address\_2>>  
 <<city>>, <<state\_province>> <<postal\_code>>  
 <<country >>

**RE: Notice of Data Breach**

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Thank you for your past and continuing support of Delaware Nature Society. Your commitment to nature and the outdoors makes our work possible.

Delaware Nature Society writes to inform you of a cyber incident that may affect the privacy of some of your information. Recently many non-profits, including Delaware Nature Society were informed by Blackbaud, Inc. (“Blackbaud”) that their system was illegally accessed by an outside party. Blackbaud is our vendor for some customer service and financial information. We are providing additional information below. Blackbaud reported that this incident **did not involve** your Social Security numbers or credit card information. **However, it did involve program registrants’ name and health insurance, allergy, or medical information.**

On Thursday, July 16, 2020, Delaware Nature Society received notification from Blackbaud of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Delaware Nature Society. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Delaware Nature Society data. This notice provides information regarding the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

**What Happened?** Blackbaud experienced a ransomware incident in May 2020 that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Delaware Nature Society immediately began to determine what, if any, sensitive Delaware Nature Society data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident.

**What Information Was Involved?** Blackbaud reported to us that this incident did not involve information such as Social Security numbers or credit card information, as this information is typically stored in encrypted fields. Moreover, Social Security numbers and credit card information are not stored by Delaware Nature Society in this system. However, in an abundance of caution, we continue to investigate to confirm Blackbaud’s assurances and better understand what occurred. Unencrypted information that may have been included on Blackbaud’s systems at the time of the incident and which may have been exposed includes your name and health insurance, allergy, or medical information.

<p><b>PRESIDENT</b> Dawn Rittenhouse</p> <p><b>VICE PRESIDENT</b> Eric Brinsfield</p> <p><b>TREASURER</b> Adele McIntosh</p> <p><b>SECRETARY</b> Nicki Taylor</p>	<p><b>EXECUTIVE DIRECTOR</b> Anne Harper</p> <p><b>DEPUTY DIRECTOR/ CHIEF DEVELOPMENT OFFICER</b> Joanne McGeoch</p>	<p><b>BOARD OF DIRECTORS</b></p> <p>Dan Barbato Mark Carter Kevin Donnelly Pamela S.Finkelman JJ Francis Barbara Greenewalt Frederick deL Greenewalt</p>	<p>Jeffrey Haas Ellen Kohler Blair McConnel Mary Y. Peck Suzanne Smith Roland Wall Marian R. Young</p>	<p><b>HONORARY DIRECTORS</b></p> <p>Bernard Dempsey Lorraine M. Fleming Peter H. Flint Nancy Frederick Michael E. Riska Norman G. Wilder* Lynn Williams * Deceased</p>
---	--	--	--	--

**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 policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

**What You Can Do.** We 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.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or need assistance, please email [datasecurity@delnature.org](mailto:datasecurity@delnature.org) or call (302) 239-2334.

Sincerely,



Anne Harper  
Executive Director

## ***Steps You Can Take to Help Protect Your Information***

### **Monitor Your 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](http://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.

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**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://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**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://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](http://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. This notice has not been delayed by law enforcement.

**For Maryland residents,** the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and [www.oag.state.md.us](http://www.oag.state.md.us).



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
 <<address\_1>>  
 <<address\_2>>  
 <<city>>, <<state\_province>> <<postal\_code>>  
 <<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Thank you for your past and continuing support of Delaware Nature Society. Your commitment to nature and the outdoors makes our work possible.

Delaware Nature Society writes to inform you of a cyber incident that may affect the privacy of some of your information. Recently many non-profits, including Delaware Nature Society, were informed by Blackbaud, Inc. (“Blackbaud”) that their system was illegally accessed by an outside party. Blackbaud is our vendor for some customer service and financial information. During a hacking incident, your bank account information, in the form of a copy of your donation check, may have been disclosed to a third party. We are providing additional information below. Blackbaud reported to us that this incident **did not involve** your Social Security numbers or credit card information.

On Thursday, July 16, 2020, Delaware Nature Society received notification from Blackbaud of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Delaware Nature Society. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Delaware Nature Society data. This notice provides information regarding the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

**What Happened?** Blackbaud experienced a ransomware incident in May 2020 that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Delaware Nature Society immediately began to determine what, if any, sensitive Delaware Nature Society data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident.

**What Information Was Involved?** Blackbaud reported to us that this incident did not involve information such as Social Security numbers or credit card information. Moreover, Social Security numbers and credit card information are not stored by Delaware Nature Society in this system. However, in an abundance of caution, we continue to investigate to confirm Blackbaud’s assurances and better understand what occurred. **Please note, although such information is typically stored in encrypted data fields, our investigation determined that the impacted Blackbaud systems contained your unencrypted name and bank account information in the form of a scanned image of a check.**

<b>PRESIDENT</b> Dawn Rittenhouse <b>VICE PRESIDENT</b> Eric Brinsfield <b>TREASURER</b> Adele McIntosh <b>SECRETARY</b> Nicki Taylor	<b>EXECUTIVE DIRECTOR</b> Anne Harper <b>DEPUTY DIRECTOR/          CHIEF DEVELOPMENT          OFFICER</b> Joanne McGeoch	<b>BOARD OF DIRECTORS</b> Dan Barbato Mark Carter Kevin Donnelly Pamela S.Finkelman JJ Francis Barbara Greenewalt Frederick deL Greenewalt	Jeffrey Haas Ellen Kohler Blair McConnel Mary Y. Peck Suzanne Smith Roland Wall Marian R. Young	<b>HONORARY DIRECTORS</b> Bernard Dempsey Lorraine M. Fleming Peter H. Flint Nancy Frederick Michael E. Riska Norman G. Wilder* Lynn Williams * Deceased
--	---	---	---	--



**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 policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

**What You Can Do.** We 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.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or need assistance, please email [datasecurity@delnature.org](mailto:datasecurity@delnature.org) or call (302) 239-2334.

Sincerely,



Anne Harper  
Executive Director

## ***Steps You Can Take to Help Protect Your Information***

### **Monitor Your 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](http://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.

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**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://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**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://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](http://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. This notice has not been delayed by law enforcement.

**For Maryland residents**, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and [www.oag.state.md.us](http://www.oag.state.md.us).