EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to this submission. By providing this notice, IFB Solutions does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, IFB Solutions a received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud advised that it reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, and two months after the incident, Blackbaud notified its customers, including IFB Solutions, that an unknown actor may have accessed or acquired certain Blackbaud customer data at some point before Blackbaud locked the actor out of its environment on May 20, 2020. According to Blackbaud, it detected the first indicator of compromise on May 14, 2020 and that unauthorized activity was contained and stopped by May 20, 2020.

Upon learning of the Blackbaud incident, IFB Solutions commenced an investigation to determine what, if any, sensitive IFB Solutions data was potentially involved. On or about September 29, 2020, IFB Solutions received additional information from Blackbaud on the incident. Because Blackbaud failed to provide a list of the potentially affected IFB Solutions data, IFB Solutions undertook a comprehensive analysis of the information Blackbaud provided and the data stored on the systems identified by Blackbaud to confirm what records could have been accessible to the threat actor and to identify the individuals associated with the records. On or about November 17, 2020, IFB Solutions completed its investigation and confirmed that personal information could have been subject to unauthorized access or acquisition including name and financial account information.

Notice to Maine Residents

On December 22, 2020, IFB Solutions provided written notice of the Blackbaud incident to two (2) Maine residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***. To date, IFB Solutions has not received any information from Blackbaud that any IFB Solutions information was specifically accessed or acquired by the unknown actor.

Other Steps Taken and To Be Taken

Upon discovering the event, IFB Solutions moved quickly to obtain information from Blackbaud regarding their incident. IFB Solutions then provided notice to potentially affected individuals associated with IFB Solutions. That notice provided information about the Blackbaud incident, IFB Solution's response thereto, and resources available to help protect personal information from possible misuse. IFB Solutions is working to review existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, IFB Solutions is providing notified individuals with guidance on how to better protect against identity theft and fraud. IFB Solutions is providing individuals with 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. IFB Solutions will also be notifying other state regulators as required.

EXHIBIT A

Winston-Salem, North Carolina
O 336.759.0551 F 336-759-0990
7730 North Point Drive, Winston-Salem, NC 27106
IFBSolutions.org

[Date]

[Name]
[Street Address]
[City, State, Zip Code]

Re: Notice of Data Breach

Dear [Name]:

Winston-Salem Industries for the Blind, Inc. dba IFB Solutions ("IFB Solutions") writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, IFB Solutions 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 IFB Solutions. 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 IFB Solutions data. This notice provides information about 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 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. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data at some point before Blackbaud locked the actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, IFB Solutions commenced an investigation to determine what, if any, sensitive IFB Solutions data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. Accordingly, in September, a preliminary message was sent to those individuals in our database in the interest of transparency providing information regarding the incident based on what we knew at that time.

Furthermore, on or about September 29, 2020, IFB Solutions received additional information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information. IFB Solutions then concluded an internal review to determine the impact to individuals' personal information and locate contact information for those affected by this incident.

What Information was Involved? Our investigation determined that the involved Blackbaud systems contained your name and financial information, which was contained on images of donor checks gifted to IFB Solutions. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

What We Are 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

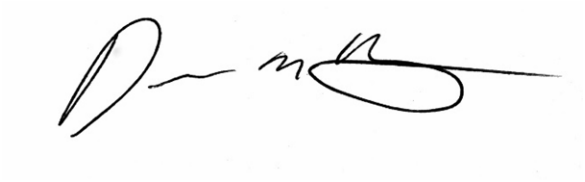
security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying regulators, as required.

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 the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 336-245-5655 between the hours of 9 a.m. to 5 p.m. EST.

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

Sincerely,



David Horton
President & CEO
IFB Solutions, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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.

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.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.