MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 19, 2020

VIA FIRST-CLASS MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Avant Technology, a subsidiary of All Components, Inc. ("Avant"), and write to notify your Office of an incident that may affect the privacy of information relating to approximately two (2) New Hampshire residents. The investigation into this incident is ongoing and Avant will supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, Avant does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

In April 2020, Avant discovered unusual activity on its network and immediately commenced an investigation to determine the nature and scope of the activity and to confirm the security of its network. The investigation, which included working with third-party forensic computer specialists, determined that Avant's network had been infected with malware that encrypted certain systems and disrupted company operations. On or around June 4, 2020, the investigation confirmed that Avant's network had been subject to unauthorized access from April 20 to April 22, 2020 and again on April 27, 2020. The investigation also determined that certain documents stored within Avant's environment could have been subject to unauthorized access or acquisition during those periods.

On June 23, 2020, the investigation confirmed the exact locations on Avant's network that were accessible during the period of unauthorized access. Because the investigation could not rule out access to information contained in these locations, Avant conducted a comprehensive review of the items to determine what information was present at the time of the unauthorized activity. On July 21, 2020, Avant completed this review and confirmed the identities of the individuals with personal information that could have been subject to unauthorized access, including two (2) New Hampshire residents. While the information impacted varies by individual, the investigation revealed the following personal information related to New

Hampshire residents was accessible to an unauthorized actor as a result of this event: Social Security Number. To date, Avant is unaware of any actual or attempted misuse of any personal information.

Notice to New Hampshire Residents

On or about August 19, 2020, Avant began providing written notice of this incident to potentially affected individuals, which includes approximately two (2) New Hampshire 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

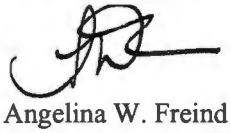
Upon discovering suspicious activity on its network. Avant moved quickly to investigate and to confirm the nature and scope of the activity. Since that time, Avant has worked tirelessly to ensure the security and stability of its network and all data contained thereon, including with computer forensic specialists to confirm the unauthorized actor's activity and to identify any risk to data on the network. Upon confirmation of unauthorized access to certain folders and documents, Avant immediately undertook a comprehensive review of the contents of these folders and documents to determine whether and what personal information may have been present. In response to this incident, Avant also took steps to ensure the security of its network, including resetting account passwords and implementing additional security measures to detect unauthorized activity.

Avant is also providing all potentially impacted individuals with notice of this incident and guidance on how to better protect against identity theft and fraud, including providing 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. As an added precaution, Avant is offering potentially affected individuals access to credit monitoring and identity theft protection service for 12 months at no cost. As part of its ongoing commitment to information security, Avant is also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,



Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/rhb

Exhibit A

<<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>>,

Avant Technology, a subsidiary of All Components, Inc. ("Avant"), writes to notify you of a recent incident that may affect the privacy of some of your personal information. *While we have no evidence of actual or attempted misuse of your information as a result of this incident,* this letter provides details about the incident, our response, and resources available to you to help protect your information should you feel it appropriate to do so.

What Happened? In April 2020, Avant discovered unusual activity on its network and immediately commenced an investigation to determine the nature and scope of the activity and to confirm the security of its network. The investigation, which included working with third-party forensic computer specialists, determined that Avant's network had been infected with malware that encrypted certain systems and disrupted company operations. On or around June 4, 2020, the investigation confirmed that Avant's network had been subject to unauthorized access from April 20 to April 22, 2020 and again on April 27, 2020. The investigation also determined that certain documents stored within Avant's environment could have been subject to unauthorized access or acquisition during those periods.

On June 23, 2020, the investigation confirmed the exact documents stored on Avant's network that were accessible during the period of unauthorized access. Because the investigation could not rule out access to information contained in these documents we conducted a thorough review of the items to determine what information was present at the time of the unauthorized activity. On July 21, 2020, we completed this review and determined your information could have been subject to unauthorized access.

What Information Was Involved? Our investigation determined your <<b2b_text_1(ImpactedData)>>, were present in the relevant documents and may have been accessible to an unauthorized actor for a limited period of time. Again, we are unaware of any actual or attempted misuse of your information.

What We Are Doing. The privacy and security of information are among our highest priorities and we have strict security measures in place to safeguard information in our care. Upon learning of unusual activity, we moved quickly to investigate and to respond to this incident and to confirm the security of our entire environment. Our response included taking steps to further secure our environment, working with third-party forensic computer specialists, and reviewing the impacted documents to determine whether and what personal information was present and could have been subject to unauthorized access. As part of our ongoing commitment to information security, we are also reviewing and enhancing existing policies and procedures related to data privacy.

Although we are unaware of any actual or attempted misuse of your personal information, we are offering you access to 12 months of identity monitoring services through Kroll at no cost to you as an added precaution. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Your Information*. We encourage you to activate these services as we are unable to act on your behalf to do so.

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. Please also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at 1-???-???-???? 8:00 am to 5:30 pm Central Time Monday through Friday (excluding some U.S. national holidays). You may also write to Avant at 828 New Meister Lane, Suite 300, Pflugerville, TX 78660.

Sincerely,

AVANT TECHNOLOGY

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people with identity protection. Your identity monitoring services[1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **November 20, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

If you have questions, please call 1-???-???-????, 8:00 am to 5:30 pm Central Time, Monday through Friday (excluding some U.S. national holidays) beginning on June 1st.

Your Identity Monitoring Services Include:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data – for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Accounts

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 listed below 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 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-680-72898	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;

[1]Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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

You can further educate yourself regarding identity theft prevention, 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. 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; 1-888-743-0023; or www.oag.state.md.us.

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/.