

17598

Artech  
Logo/LetterHead

[First Name] [Last Name]  
[Address]  
[City], [State] [Zip]

[Date]

Dear [Name]:

Artech, LLC (“Artech”) is writing to inform you of an incident that could affect the security of some of your information. While we are unaware of any actual or attempted misuse of your information as a result of this incident, we take this incident very seriously and we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

Artech is committed to protecting the confidentiality and security of all the information we hold in our care. After learning of this incident, we launched an investigation with the assistance third party forensic investigators. Artech has security measures in place to protect the data in our care and we are reviewing these measures as part of our ongoing commitment to the security of that information.

As an added precaution, we are also offering you access to 24 months of identity monitoring services through Kroll at no cost to you. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. If you wish to activate these identity monitoring services, you may follow the instructions included below.

**To Enroll:**

Visit <<**IDMonitoringURL**>> to activate and take advantage of your identity monitoring services.

*You have until <<**Date**>> to activate your identity monitoring services.*

Membership Number: <<**Member ID**>>

**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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

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  
[https://www.transunion.com/  
fraud-alerts](https://www.transunion.com/fraud-alerts)

**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)

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). 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 (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement, the FTC, and the Massachusetts Attorney General.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at ###-###-### between 8:00 a.m. and 5:30 p.m. Central Time Monday through Friday excluding major U.S. holidays.

Sincerely,

[name]

[title]

Artech, LLC

# EXHIBIT B

## NOTICE OF DATA EVENT

[Date]

Artech, LLC (“Artech”) is posting the following statement to inform individuals of an event that could potentially affect the security of certain information.

**What Happened?** On January 8, 2020, Artech received a report of unusual activity relating to an employee’s Artech user account. Artech immediately began investigating this report and through that investigation identified ransomware on certain Artech systems. That same day Artech engaged a leading third-party forensic investigation firm to assess the security of its systems and to confirm the nature and scope of the incident. On January 15, 2020, the investigation determined that an unauthorized actor had access to certain Artech systems between January 5, 2020, and January 8, 2020. Artech undertook a comprehensive review of these systems and determined that some personal information was present in them at the time of the incident. Artech reviewed this information and its internal records to identify the individuals associated with this information and their contact information for purposes of providing notice. On or around June 25, 2020, we completed this review and determined that personal information relating to certain individuals was contained in one or more of the involved files.

**What Information Was Involved?** The investigation determined that at the time of the incident the involved files may have contained information including name, Social Security number, medical information, health insurance information, financial information, payment card information, driver’s license/state identification number, government issued identification number, passport number, visa number, electronic/digital signature, username and password information. The information varied by individual. To date, Artech is unaware of any actual or attempted misuse of personal information as a result of this incident.

**What Artech Is Doing.** Artech takes this incident and the security of personal information in its care very seriously. Upon learning of this incident, Artech immediately commenced an investigation using external digital forensic specialists, changed system credentials and took steps to secure its systems and assess relevant company systems that may have been impacted by the event. Artech is also working with external digital forensic specialists to enhance existing security processes and protocols.

Individuals who were determined to be potentially impacted by this event will receive written notice of the event by mail if a valid address existed.

**What Can You Do?** Artech encourages individuals to remain vigilant against incidents of identity theft and fraud and to review account statements for suspicious activity.

Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, individuals may visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of a credit report.

Individuals have the right to place a “security freeze” on a credit report, which will prohibit a consumer reporting agency from releasing information in a credit report without express authorization. The security

freeze is designed to prevent credit, loans, and services from being approved in a person's name without consent. However, be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application a person makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, a person cannot be charged to place or lift a security freeze on a credit report. Should a person wish to place a security freeze, they may 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, individuals will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If a person has moved in the past five (5) years, the addresses they 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 a person is the victim of identity theft, 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, individuals have the right to place an initial or extended "fraud alert" on a 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 an individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should a person wish to place a fraud alert, they may 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-alerts](http://www.transunion.com/fraud-alerts)

**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)

Individuals can obtain additional information regarding identity theft, fraud alerts, security freezes, and the steps that can be taken to protect themselves by contacting the consumer reporting agencies, the Federal Trade Commission, or the individual's relevant 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.

***For More Information.*** Artech understands that you may have questions about this incident that are not addressed in this statement. If you have additional questions or would like to confirm if you are affected by this event, please call the dedicated assistance line at ~~###-###-####~~ between 8:00 am and 5:30 pm Central Time Monday through Friday, excluding major U.S. holidays.



# EXHIBIT C

## PRESS RELEASE

**Morristown, New Jersey** – Artech, LLC (“Artech”) today announced that it is notifying potentially affected individuals of a recent data security incident that could potentially impact the security of certain personally identifiable information (personal information).

While Artech is unaware of any actual or attempted misuse of personal information as a result of this incident, the company is notifying potentially affected individuals to provide information about the incident and access to resources to protect their information, should they feel it is appropriate to do so. Artech takes this incident and the security of personal information in our care seriously.

***What Happened?*** On January 8, 2020, Artech received a report of unusual activity relating to an employee’s Artech user account. Artech immediately began investigating this report and through that investigation identified ransomware on certain Artech systems. That same day Artech engaged a leading third-party forensic investigation firm to assess the security of its systems and to confirm the nature and scope of the incident. On January 15, 2020, the investigation determined that an unauthorized actor had access to certain Artech systems between January 5, 2020 and January 8, 2020. Artech undertook a comprehensive review of these systems and determined that some personal information was present in them at the time of the incident. Artech reviewed this information and its internal records to identify the individuals associated with this information and their contact information for purposes of providing notice. On or around June 25, 2020, we completed this review and determined that personal information relating to certain individuals was contained in one or more of the involved files.

***What Information Was Involved?*** The investigation determined that at the time of the incident the involved files may have contained information including name, Social Security number, medical information, health insurance information, financial information, payment card information, driver’s license/state identification number, government issued identification number, passport number, visa number, electronic/digital signature, username and password information. The information varied by individual. To date, Artech is unaware of any actual or attempted misuse of personal information as a result of this incident.

***What Artech Is Doing.*** Artech takes this incident and the security of personal information in its care very seriously. Upon learning of this incident, Artech immediately commenced an investigation using external digital forensic specialists, changed system credentials and took steps to secure its systems and assess relevant company systems that may have been impacted by the event. Artech is also working with external digital forensic specialists to enhance existing security processes and protocols.

Individuals who were determined to be potentially impacted by this event will receive written notice of the event by mail if a valid address existed.

***What Can You Do?*** Artech encourages individuals to remain vigilant against incidents of identity theft and fraud and to review account statements for suspicious activity.

Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, individuals may visit

[www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of a credit report.

Individuals have the right to place a "security freeze" on a credit report, which will prohibit a consumer reporting agency from releasing information in a credit report without express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in a person's name without consent. However, be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application a person makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, a person cannot be charged to place or lift a security freeze on a credit report. Should a person wish to place a security freeze, they may 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, individuals will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If a person has moved in the past five (5) years, the addresses they 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 a person is the victim of identity theft, 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, individuals have the right to place an initial or extended "fraud alert" on a 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 an individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should a person wish to place a fraud alert, they may 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-alerts](http://www.transunion.com/fraud-alerts)

**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)

Individuals can obtain additional information regarding identity theft, fraud alerts, security freezes, and the steps that can be taken to protect themselves by contacting the consumer reporting agencies, the Federal Trade Commission, or the individual's relevant 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.

***For More Information.*** Artech understands that you may have questions about this incident that are not addressed in this statement. If you have additional questions or would like to confirm if you are affected by this event, please call the dedicated assistance line at ###-###-#### between 8:00 am and 5:30 pm Central Time Monday through Friday excluding major U.S. holidays.