SMITH

March 5, 2021

Washington State Office of the Attorney General
800 5th Ave., Suite 2000
Seattle, WA 98104

RE: Ascentium Inc. and Ascentium Corp. (SMITH)
FEIN No. 91-2105883
Notification of Data Security Breach (Ransomware Attack) 2020-12-24 Discovery & 2021-02-24 Discovery of Data on Dark Web

On behalf of Ascentium Inc. and Ascentium Corp. (SMITH), in an abundance of caution, we are providing notice of a ransomware attack (notice of a data security breach) on Canadian server(s) which contained legacy employee personal identifying information for current and some former employees located in the United States. 172 employee(s) in the State of Washington was/were affected.

What Happened. On December 24, 2020, SMITH was alerted to a ransomware attack to SMITH's onsite server which contained current and legacy employee personal identifying information. Ransomware is destructive malware that encrypts or corrupts data. The number of total current and former employees whose legacy data was encrypted is approximately 1,400 within the United States footprint.

SMITH has since learned that information was extracted and that, on or about February 24, 2021, the extracted files were uploaded onto the webpage on the dark web. SMITH has alerted law enforcement in Canada, where the server is located, regarding this development with the objective of protecting and securing personal information.

What Information Was Involved. The legacy employee personal identifying information which was on the server affected with ransomware may have included a combination of two or more of the following types of information: name, address, phone, email, social security number, driver's license number and/or payroll information.

What We Did and Are Doing in Response to The Incident. SMITH took immediate steps to address this matter and to prevent future similar incidents from occurring. SMITH took the servers upon which ransomware was installed offline that same day. SMITH engaged its third-party IT Security vendor to assist SMITH in assessing both potential exposure and mitigation strategies. By December 25, 2020, all networks admin users and passwords were reset. Subsequently, all employee and contractor passwords have been reset. SMITH is restoring any necessary data from unaffected backup sources. In addition, most employee data is now housed via third party sources.

SMITH engaged Equifax to distribute the attached original notice. **Exhibit 1 (Original Sample Notice).** Formal Notice was mailed by Equifax on February 8, 2021. SMITH offered a complimentary two-year credit monitoring membership to Equifax.

Smith retained an outside cybersecurity vendor to identify additional preventative measures that SMITH can implement.

SMITH

When data was discovered on the dark web on February 24, 2021, as described above, SMITH engaged Equifax to distribute the attached supplemental notice regarding discovery that the data was on the dark web on or about March 1, 2021. **Exhibit 2 (Supplemental Sample Notice).**

For further information, please contact counsel Frederic Dorwart Lawyers, PLLC by emailing edorwart@fdlaw.com.

Sincerely,

Ascentium Inc. and Ascentium Corp. (SMITH)

3601 Rigby Rd, Suite 420
Miamisburg, OH 45342

SMITH

NOTICE OF DATA SECURITY BREACH

February 3, 2021

[First Name] [Last Name]
[Address 1], [Address 2]
[City], [State] [Zip]

Dear [First Name],

At Ascentium Corp. (SMITH), we place a high value on earning your trust and continuing to preserve that trust. On behalf of SMITH, we are providing notice to you of a ransomware attack (notice of a data security breach) on server(s) which contained legacy employee personal identifying information for current and some former employees.

What Happened. On December 24, 2020, SMITH was alerted to a ransomware attack to SMITH's onsite server which contained current and legacy employee personal identifying information. Ransomware is destructive malware that encrypts or corrupts data.

What Information Was Involved. The legacy employee personal identifying information which was on the server affected with ransomware may have included a combination of two or more of the following types of information: name, address, phone, email, social security number, driver's license number and/or payroll information. Your personal information was located on the server that was ransomed.

What We Did And Are Doing In Response To The Incident. SMITH took the servers upon which ransomware was installed offline that same day. SMITH engaged its third-party IT Security vendor to assist in assessing potential exposure and implementing mitigation strategies.

What You Can Do. SMITH offering a complimentary two-year membership to Equifax, which provides credit monitoring for three major credit monitoring bureaus, protection of your personal information and identity theft insurance:

Equifax ID Patrol® provides you with the following key features:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- Automatic Fraud Alerts. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).
- Credit Report Lock Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.

SMITH

- Internet Scanning Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID
- Up to $1 MM in identity theft insurance
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/patrol

1. Welcome Page: Enter your unique Activation Code of [Activation Code] and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept and click the "Continue" button.

4. **Verify ID**: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

SMITH encourages you to:

- Review the information provided in the websites listed below in the For More Information Section and take appropriate action;
- Review security steps that may be taken with each of your financial institutions;
- If appropriate, place extended fraud alerts with the three major credit monitoring bureaus

For More Information.

The FDIC has helpful information regarding steps to take in the event confidential information has been out of your control or the Bank's control. Please see: http://www.fdic.gov/consumers/theft/. *See also,* the FDIC's article, which can be accessed via the following link: http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf The FTC (Federal Trade Commission) also provides helpful information regarding steps to take in the event banking information has been out of your control or the Bank's control. Please see: http://www.consumer.ftc.gov/topics/privacy-identity. If you or an individual suspects that he/she/they/it is the victim of identity theft, contact the Federal Trade Commission at 1-877- ID-THEFT.

For customer convenience, we have provided contact information for the three major credit monitoring bureaus by way of the website links above and the table below.

SMITH

Equifax	Experian	TransUnion	Source
800-685-1111	888-397-3742	800-680-7289	http://business.ftc.gov/documents/bus59-information-compromise-and-risk-id-theft-guidance-your-business
800-525-6285	888-397-3742	800-680-7289	http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf
www.equifax.com	www.experian.com	www.transunion.com	http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

We have resources available to answer your questions and provide additional information to you. Please call 866-349-3221 if you have any further questions.

We again sincerely apologize for any potential inconvenience and/or worry that this ransomware attack on SMITH's servers and legacy data may have caused.

Sincerely,

SMITH

SMITH

SUPPLEMENT TO FEBRUARY 3, 2021
NOTICE OF DATA SECURITY BREACH

February 26, 2021

[First Name] [Last Name]
[Address 1], [Address 2]
[City], [State] [Zip]

Dear [First Name],

At Ascentium Corp. (SMITH), we place a high value on earning your trust and continuing to preserve that trust. This is why we are writing to update you regarding the ransomware attack that we notified you about in our letter of February 3, 2021. For your convenience, we enclose another copy of our original letter. (Exhibit 1).

When we previously notified you of the data security incident, we did not have sufficient information to know whether any information had actually been extracted from our on-site server. However, we have now received confirmation that information was extracted and that, on or about February 24, 2021, the extracted files were uploaded onto the webpage on the dark web. We have alerted law enforcement regarding this development with the objective of protecting and securing your personal information.

We sincerely apologize for this incident, and wish to communicate to all affected individuals that we are taking immediate steps to address this matter and to prevent future similar incidents from occurring. For example, we have retained an outside cybersecurity vendor to identify additional preventative measures that we can implement. We have also taken steps to notify persons affected by the incident as well as attorneys general per applicable state law.

Despite these steps, we strongly encourage you to take further steps to protect yourself against potential risks associated with this incident. As noted in our previous letter, we are offering a complimentary two-year membership to Equifax, which provides credit monitoring, protection of your personal information and identity theft insurance. The details of the Equifax product and enrollment instructions are re-copied here for convenience:

Equifax ID Patrol® provides you with the following key features:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- Automatic Fraud Alerts. With a fraud alert, potential lenders are encouraged to take extrasteps to verify your ID before extending credit (available online only).
- Credit Report Lock Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.

SMITH

- Internet Scanning Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID.
- Up to $1 MM in identity theft insurance
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/patrol

1. Welcome Page: Enter your unique Activation Code of [Activation Code] and click the"Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, dateof birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept and click the "Continue"button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity.Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the"View My Product" button to access the product features.

In addition to registering for the complimentary Equifax service that we have offered, below are additional ways that you can help reduce the risk of harm:

1. Regularly Review Your Credit Report

We recommend that you regularly review statements from your accounts and periodically obtain and review your credit report from Equifax, Experian or TransUnion. The contact information for these three national credit reporting agencies is as follows:

- **Equifax**
  www.equifax.com
  1-800-685-1111

- **Experian**
  www.experian.com
  1-888-397-3742

- **Transunion**
  www.transunion.com
  1-800-680-7289

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for any information that is not accurate, such as your home address or Social Security Number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

SMITH

We recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. We also recommend that you promptly report any suspicious activity or any suspected incidence of identity theft to us and to the proper law enforcement authorities, including local law enforcement and the Canadian Anti-Fraud Centre (CAFC).

2. Consider Placing Fraud Alerts on your Credit File

A fraud alert is a notice placed on your credit file that alerts creditors that you may be a victim of fraud. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting the three credit reporting bureaus listed above.

3. Consider Freezing Your Credit

Freezing your credit will not allow anyone to establish a new credit facility with your identity unless you authorize with a secure PIN. You may freeze your credit using the links below for the three national credit reporting agencies:

- **Equifax**
  https://my.equifax.com/consumer-registration/UCSC/#/personal-info
- **Experian**
  https://www.experian.com/freeze/center.html
- **TransUnion**
  https://www.transunion.com/credit-freeze

4. Additional Sources of Information about Identity Theft.

The FDIC has helpful information regarding steps to take in the event confidential information has been out of your control or the Bank's control. Please see: http://www.fdic.gov/consumers/theft/. *See also,* the FDIC's article, which can be accessed via the following link: http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf The FTC (Federal Trade Commission) also provides helpful information regarding steps to take in the event banking information has been out of your control or the Bank's control. Please see: http://www.consumer.ftc.gov/topics/privacy-identity. If you or an individual suspect that he/she/they/it is the victim of identity theft, contact the Federal Trade Commission at 1-877- ID-THEFT.

The IRS also has helpful information on steps to protect taxpayers from identify theft. Please see: https://www.irs.gov/newsroom/eight-tips-to-protect-taxpayers-from-identity-theft

SMITH

We have resources available to answer your questions and provide additional information to you. Please call 866-349-3221 if you have any further questions.

We again sincerely apologize for any potential inconvenience and/or worry that this ransomware attack on SMITH's servers and legacy data may have caused.

Sincerely,

SMITH