

NORTON ROSE FULBRIGHT

August 24, 2020

Via FedEx

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

STATE OF NH
DEPT OF JUSTICE
2020 AUG 25 PM 12:34

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I am writing on behalf of my client, VT San Antonio Aerospace, Inc. ("SAA"), to notify your office that SAA was the target of a ransomware attack that exposed the personal information of approximately twelve (12) New Hampshire residents. SAA provides comprehensive, high-quality and timely aircraft maintenance modification services for a wide range of commercial and VIP aircraft.

On May 22, 2020, SAA discovered that certain servers within its systems had been infected with ransomware. SAA immediately launched an investigation and engaged a leading cybersecurity and forensics firm to determine the nature and scope of the incident. SAA also notified the Federal Bureau of Investigation and the U.S. Department of Defense.

Shortly after the ransomware attack was launched, SAA was contacted by the Maze Group, who demanded a ransom and also claimed to have exfiltrated data from SAA's systems. The forensic investigation confirmed data was exfiltrated from the SAA environment prior to the release of the ransomware on May 22, 2020. In spite of repeated taunts and threats in an attempt to extort SAA to pay the ransom, the company refused to concede. In retaliation, the MAZE group published stolen data to the MAZE website between June 4, 2020 and July 6, 2020 in order, we believe, to provide incentive for SAA to reconsider the ransom demand.

We have conducted a thorough review of the information that has been published on the Maze Group website, as well as other files our investigation has indicated were stolen. We are now notifying the individuals whose personal data we have confirmed was exfiltrated and those whose information we have reason to believe was exfiltrated. Notification of this incident is being provided as quickly as possible, following the completion of the investigation, which was performed without unreasonable delay. We have confirmed the following types of the New Hampshire residents' personal information may have been stolen: name, Social Security number, date of birth, health information, passport number, and financial account number. Should further data be published on the Maze website, we will conduct a further thorough review of the information to determine whether any additional individuals need to be notified.

We are not aware of any fraud or misuse of any personal information as a result of this incident. We do not believe personal information was targeted by the threat actor for identity theft purpose,

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

but rather, such information happened to be included in documents taken by the threat actor as part of the ransomware attack to extort the company.

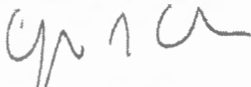
SAA continues to review its security measures, internal controls, and safeguards and continues to make changes to help prevent a similar incident from occurring in the future including but not limited to:

- engaging a specialist vendor to assist with system recovery which include vulnerability and configuration hardening actions for SAA;
- awarding a managed service contract to a third-party with qualified and certified Palo Alto engineers to improve the management of firewall protections for SAA;
- deploying advanced tools like FireEye HX technology across all SAA endpoints and servers, which are also being monitored 24x7x365 by FireEye Security Operations Centre;
- deploying enhanced FireEye network (NX/PX) and email security (ETP) protections for SAA; and
- strengthening firewalls to include hardened configurations and improved logging capabilities for SAA.

We will notify affected New Hampshire residents on August 25, 2020 and will be offering them 24 months of complimentary credit monitoring and fraud protection services. A copy of the notice letter is attached.

If you have any questions or need further information regarding this incident, please contact me at (202) 662-4691 or chris.cwalina@nortonrosefulbright.com.

Very truly yours,



Chris Cwalina

CGC/

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 25, 2020



F7304-L01-0000001 P001 T00001 *****MIXED AADC 159
SAMPLE A SAMPLE - SSN
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



RE: Notice of Data Security Incident

Dear Sample A Sample:

VT San Antonio Aerospace, Inc. (“SAA”), a subsidiary of ST Engineering North America, Inc. (formerly known as Vision Technologies Systems, Inc. or VT Systems) (“STENA”), was recently the victim of a criminal ransomware attack. We are writing to inform you that the incident may have affected your personal information. This notice describes what we know, steps we have taken in response to the incident, and additional actions you may take to protect yourself.

What Happened

SAA recently discovered it was the target of a ransomware attack. A sophisticated group of cyber criminals gained access to SAA’s systems after deploying malware across SAA’s network and stole some files from SAA’s environment (some of which were STENA files). Once SAA discovered the incident, it immediately retained a leading cybersecurity forensics firm to help conduct a thorough investigation of the incident. SAA also reported the incident to, and is working closely with, the Federal Bureau of Investigation (“FBI”). The investigation revealed that some of your personal information was contained in the stolen files.

What Information Was Involved

The personal information contained in the stolen files may include your name and one or more of the following: social security number, driver’s license number, passport number, other government-issued identification number and information, for example, a foreign government-issued identification and/or a U.S. visa, financial account or routing number, credit/debit card number, date of birth, and/or health information.

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. We take the protection of your information very seriously. We have also implemented additional security protocols designed to protect our network and systems to prevent a similar type of incident from occurring in the future.

VT San Antonio Aerospace, Inc.
9800 John Saunders Road
San Antonio, Texas, 78216

www.stengg.com



In addition, to help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: November 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 by **November 30, 2020**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 24-Month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks, and the 24-month service is offered at no cost to you.

You can contact Experian **immediately** regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit- and non-credit-related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic funds transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do

We also recommend that you remain vigilant with respect to reviewing your account statements and credit reports and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the U.S. Federal Trade Commission ("**FTC**"). Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the FTC regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information

The security of your personal information is important to us, and we sincerely regret that this incident occurred. For more information, please contact us: by email at STENASecurity@stengg.us or by phone at (833) 902-2941, Monday through Friday, 9:00 a.m. to 5:00 p.m. Eastern time.

Sincerely,



Stephen Lim
President, VT San Antonio Aerospace, Inc.
Chief Operating Officer, ST Engineering North America, Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000001



F7304-L01

Information About Identity Theft Protection

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("**FTC**") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one (1) business day. If you request a lift of the freeze, the agency must lift it within one (1) hour. If you make your request by mail, the agency must place or lift the freeze within three (3) business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of ninety (90) days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. 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); TTY: 1-866-653-4261. The FTC 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.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York State Attorney General's Office, Consumer Frauds & Protection Bureau, 120 Broadway – 3rd Floor, New York, NY 10271, <https://ag.ny.gov/bureau/consumer-frauds-bureau>, 1-800-771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400

Obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the FTC, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.



