



March 23, 2022

By Email

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov
attorneygeneral@doj.nh.gov

Orrick, Herrington & Sutcliffe LLP
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097
+1 206 839 4300
orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

Re: Notice of Data Security Event Relating to New Hampshire / Superior Plus

Dear Attorney General:

On December 13, 2021, Superior Plus Corp. (“Superior Plus”) was alerted to a ransomware attack that encrypted various servers and business applications in Superior Plus’ IT environment. Immediately after detecting unauthorized access to our systems, we took steps to shut down the unauthorized access, restore systems to minimize disruption to Company operations, and enhance security controls across our Company. Leading cybersecurity firms were engaged to assist us in our investigation into what happened, what data was impacted, and to whom the data belongs. Superior Plus also notified U.S. and Canadian law enforcement.

After completing a thorough analysis of the data, Superior Plus has determined that 328 of New Hampshire’s residents were impacted by this data event. Although the exact information impacted varies from individual to individual, the personal information impacted includes names, driver’s license numbers, phone numbers, addresses, government identification numbers, Social Security Numbers, dates of birth, financial account numbers, credit or debit card numbers, insurance information, and limited health information. We are sending these impacted individuals notice letters via U.S. Postal Service on March 25, 2022. A sample individual notice letter is attached as Exhibit A.

Superior Plus is committed to safeguarding confidential and sensitive information. Superior Plus is offering two years of credit monitoring and identity theft protection insurance and restoration services to individuals whose sensitive information has been impacted through our preferred third-party vendor, TransUnion.



Office of the Attorney General
March 23, 2022
Page 2

In addition to these actions, Superior Plus has taken additional steps to enhance our security program, including reinforcing our security practices and is actively reviewing our systems to enhance security monitoring and controls, and to fortify the same. And, as part of our ongoing security operations, we regularly review our security and privacy policies and procedures and implement changes when needed to enhance our information security and privacy programs and controls.

If your office requires any further information in this matter, please contact me at 206-839-4340 or aswaminathan@orrick.com.

Sincerely,

A handwritten signature in black ink, appearing to read "ASW". The signature is fluid and cursive, with the letters connected.

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe LLP

EXHIBIT A

Superior Plus Propane
P.O. Box 3923
Syracuse, NY 13220



[REDACTED]

March 25, 2022

Re: Notice of Cybersecurity Event

[REDACTED],

Superior Plus recently experienced a cybersecurity event. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on what you can do and how you can obtain free credit monitoring and identity theft protection.

What happened?

On December 13, 2021, Superior Plus detected a security matter involving unauthorized access to portions of our IT systems. Immediately after detecting unauthorized access to our systems, we took steps to shut down the unauthorized access, restore systems to minimize disruption to Company operations, and enhance security controls across our Company. Leading cybersecurity firms were engaged to assist us in our investigation into what happened, what data was impacted, and to whom the data belongs.

What information was involved?

We want to notify you that we have determined that some of your personal information was accessed and/or acquired without authorization. This information falls into the following categories of data: employee identification number, credit or debit card number.

What we are doing:

Superior Plus is committed to safeguarding confidential and sensitive information. Superior Plus is offering two years of credit monitoring and identity theft protection insurance and restoration services through our preferred third-party vendor, Cyberscout. This is at no cost to you.

Please see Attachment A for details regarding these services, as well as how to enroll with your unique code. If you would like to obtain these services, please visit <https://www.myidmanager.com>. You must enroll by July 31, 2022, to receive these services and insurance.

In addition to these actions, Superior Plus has taken additional steps to enhance our security program, including reinforcing our security practices and is actively reviewing our systems to enhance security monitoring and controls, and to fortify the same. And, as part of our ongoing security operations, we regularly review our security and privacy policies and procedures and implement changes when needed to enhance our information security and privacy programs and controls.

Superior Plus Corp.

401-200 Wellington Street West
Toronto, Ontario M5V 3C7

Tel: 416-345-8050
Fax: 416-340-6030

Toll Free: 866-490-PLUS
Web: www.superiorplus.com

What you can do:

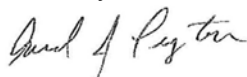
In addition to enrolling in the credit monitoring and identity theft protection insurance and restoration services being offered to you at no charge, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in Attachment B.
- It is always a good idea to be alert for “phishing” emails by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, government identification numbers, or bank account information.

For more information:

Superior Plus has established a dedicated call center to answer questions about the cybersecurity event as well as the CyberScout services that we are offering to you. If you have any questions, please call the call center at 1-800-405-6108, Monday through Friday from 8:00 a.m. to 8:00 p.m. ET, except holidays. Representatives are available for 90 days.

Sincerely,



Andy Peyton
President, Superior Plus Propane

Attachment A – CyberScout Instructions

Activation Code: I0tzjuoru3gt

We have retained the assistance of Cyberscout, a company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged access to Credit Monitoring services*, at no cost to you. Cyberscout has been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and placing fraud alerts.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

You will be prompted to enter the following activation code:

Please ensure that you redeem your activation code before take advantage of the service.

Upon your completion of the enrollment process, you will have access to the following features:

- Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- Identity theft insurance of up to \$1,000,000 in coverage to protect against potential damages related to identity theft and fraud.
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-800-405-6108.

Attachment B – Information for U.S. Residents

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

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, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the 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.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800)-771-7755; or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.