MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

July 07, 2021

VIA U.S. 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 East Coast Seafood Group LLC ("East Coast") located at 10 N Front St., New Bedford, MA 02740, and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately eighteen (18) New Hampshire residents. This notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, East Coast 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

On December 3, 2020, East Coast discovered that its network had been impacted by a malware attack that encrypted certain systems. East Coast immediately launched an investigation to determine the nature and scope of the event. East Coast quickly worked to: (1) secure the systems; (2) restore access to the information so it could continue to operate without disruption and (3) investigate what happened and whether this resulted in any unauthorized access to, or theft of, information by the unknown actor. East Coast also notified federal law enforcement. Through its investigation, East Coast determined that the unknown actor gained access to certain systems between November 10, 2020 and December 4, 2020, and certain data was exfiltrated from their systems. Some of this data was posted by the unknown actor on December 10, 2020.

East Coast then worked with third-party specialists to perform a comprehensive programmatic and manual review of information stored on the impacted systems and posted by the unknown actor to determine what information was affected and to whom the information related. Upon completion of the third-party review, East Coast then conducted a manual review of its records to determine the

identities and contact information for potentially impacted individuals. East Coast recently confirmed address information for affected individuals to provide notifications.

The impacted information varies by individual and for New Hampshire residents includes name, address, Social Security number and driver's license number.

Notice to New Hampshire Residents

On December 29, 2021, East Coast provided preliminary notice of this event and complimentary credit monitoring services to potentially affected employees while the investigation was underway. On July 7, 2021, East Coast continued providing written notice of this incident to affected individuals, which includes approximately eighteen (18) 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 the event, East Coast moved quickly to investigate and respond to the incident, assess the security of East Coast systems, and notify potentially affected individuals. East Coast is also working to implement additional safeguards and training to its employees. East Coast is providing access to credit monitoring and identity restoration services for 24 months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. East Coast also established a dedicated telephone assistance line to address questions or concerns from notified individuals.

Additionally, East Coast is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. East Coast is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/acs

EXHIBIT A

EAST COAST SEAFOOD
GROUP

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Breach

Dear <<first_name>> <<last_name>>:

East Coast Seafood Group ("East Coast") is writing to inform you of a recent event that may impact the security of some of your information. While we have received no indications of actual misuse of information as a result of this event, this notice provides information about the event, our response and efforts to secure our environment, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On December 3, 2020, East Coast discovered that its network had been impacted by a malware attack that encrypted certain systems. East Coast immediately launched an investigation to determine the nature and scope of the event. East Coast quickly worked to: (1) secure the systems; (2) restore access to the information so it could continue to operate without disruption and (3) investigate what happened and whether this resulted in any unauthorized access to, or theft of, information by the unknown actor. Through our investigation, we determined that the unknown actor gained access to certain systems between November 10, 2020 and December 4, 2020, and certain data was exfiltrated from our systems. Some of this data was posted by the unknown actor on December 10, 2020.

We then worked with specialists to perform a comprehensive review of information stored on the impacted systems and posted by the unknown actor to determine what information was affected and to whom the information related. Upon completion of the third-party review, we then conducted a manual review of our records to determine the identities and contact information for potentially impacted individuals. Recently, we confirmed address information for affected individuals to provide notifications.

What Information Was Involved. Our investigation determined that the impacted information may have included your <<b2b_text_1(DataElements)>>.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. East Coast is reviewing its security policies and procedures to reduce the risk of similar future events. Although we do not have any indication of identity theft or fraud as a result of this incident, we are offering complimentary identity monitoring services through Kroll for 24 months as an added precaution. We also reported this event to federal law enforcement and notified state regulators, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. Additional information and resources are included in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also activate the complimentary identity monitoring services available to you. Activation instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-XXX-XXX-XXXX, Monday through Friday (excluding U.S. holidays), during the hours of 9:00 a.m. to 6:30 p.m., Eastern Time. You may also write to East Coast at 10 N Front St., New Bedford, MA 02740.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Paul Lacorazza
Chief Financial Officer
East Coast Seafood Group LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **September 23, 2021** to activate your identity monitoring services.*

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

You have been provided with access to the following services from Kroll:

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you 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. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are # Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/