

December 17, 2021

**Rachel H. Cobble, Esq.**  
205.709.8991 (direct)  
Rachel.Cobble@WilsonElser.com

Via electronic-mail: [DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov); [AttorneyGeneral@doj.nh.gov](mailto:AttorneyGeneral@doj.nh.gov)

**Attorney General John M. Formella**

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

**Re: Our Client : Seacoast Security, Inc.**  
**Matter : Data Security Incident on September 3, 2020.**  
**Wilson Elser File # : 16516.01140**

---

Dear Attorney General Formella:

We represent Seacoast Security, Inc. (“SSI”), located in West Rockport, Maine, with respect to a data security incident described in more detail below. SSI takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that SSI is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On September 3, 2020, SSI was a target of a cybersecurity attack. SSI immediately engaged third-party specialists to secure and remediate the environment, and then investigate the extent of the unauthorized activity within the network environment. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted individuals’ names, mailing addresses, dates of birth, and driver licenses could have been exposed as a result of this attack.

As of this writing, SSI has not received any reports of related identity theft since the date of the incident.

2. Number of New Hampshire Residents Affected

A total of seven (7) residents of New Hampshire were potentially affected by this security incident. Notification letters to these individuals were mailed on December 15, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, SSI contacted cybersecurity experts and a reputable third party forensic team to assist with its investigation. Although SSI is not aware of any evidence of misuse of personal information, SSI extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed id theft recovery service, should the need arise.

4. Contact Information

SSI remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Rachel.Cobble@WilsonElser.com or 205.709.8991.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Rachel H. Cobble, Esq.

Copy: Robert Walker, Esq. (Wilson Elser LLP)  
Michael E. Kar, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

Seacoast Security

10300 SW Greenburg Rd. Suite 570  
Portland, OR 97223



**SEACOAST  
SECURITY**

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:  
1-800-939-4170  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code: <<XXXXXXXXXX>>

December 15, 2021

### **Notice of Data Breach**

Dear <<First Name>> <<Last Name>>,

We are writing in order to inform you of an incident that may have exposed portions of your account information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

#### **What Happened and What Information was Involved?:**

Seacoast Security, Inc. (“SSI”) was the target of a cybersecurity incident on September 3, 2020. Upon detection, we immediately took steps to investigate and determine the nature of the incident, as well as enhance our network security measures. A comprehensive investigation was also done to identify any instances of sensitive data compromise. Although we have found no evidence that your information has been specifically misused, it is possible that your full name, mailing address, birthdate, and driver’s license could have been exposed to the cybercriminal.

We maintain this information on our system for standard administrative purposes and alarm handling.

As of this writing, SSI has not received any reports of related identity theft since the date of the incident (September 3, 2020 – present).

#### **What We Are Doing:**

Upon detecting this incident, we moved quickly to initiate our incident response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of our network environment. We have reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

#### **What You Can Do:**

We encourage you to contact IDX and to enroll in free IDX services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 9 am – 9pm Eastern Time. Please note the deadline to enroll is **March 15, 2022**.

Enclosed hereto you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

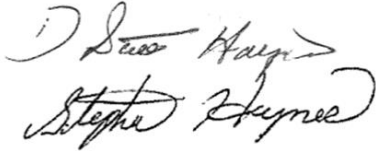
Again, at this time, there is no evidence that your information was compromised or misused. However, we encourage you to take the time to evaluate your alarm system procedures.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-800-939-4170.

Seacoast Security, Inc. values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,

Handwritten signatures of D Scott Haynes and Stephen Haynes. The signature of D Scott Haynes is written above the signature of Stephen Haynes.

---

D Scott Haynes, President  
Stephen Haynes, Vice President

### **Additional Information**

**Credit Reports:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 <a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion Security Freeze</b> P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>
---	---	--

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**File Police Report:** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**FTC and Attorneys General:** 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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), 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. This notice has not been delayed by law enforcement.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and [www.oag.state.md.us](http://www.oag.state.md.us).

**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 agencies 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 violators. 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](http://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 North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and [www.ncdoj.gov](http://www.ncdoj.gov).

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

**For Rhode Island residents**, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://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.