MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Gregory Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1127 High Ridge Road, #301
Stamford, CT 06905

August 6, 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 Ibex Global Solutions, Inc. ("Ibex") located at 310 N 2nd E #102, Rexburg, Idaho 83440, and are writing to notify your office of an incident that potentially affects the security of some personal information relating to fifty-six (56) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ibex 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 August 17, 2020, Ibex learned that it was the victim of a malware attack that impacted the availability of a limited segment of its systems. Ibex immediately took these systems offline and, with the assistance of third-party computer specialists, launched an investigation to determine the nature and scope of the incident. On or about September 15, 2020, the investigation confirmed that certain files on Ibex's systems may have been accessed without authorization between July 27 and August 17, 2020. Ibex therefore undertook a meticulous and time-intensive review of the potentially impacted files and its internal systems in order to identify the information that was involved and to whom it related. In connection with this review, on or about September 29, 2020, a third-party firm was engaged to review the potentially impacted files. Ibex, upon receiving and validating the findings of the third-party firm, on or about June 14, 2021, determined that one or more of the potentially impacted folders included information related to individuals, including name, address, Social Security number, date of birth, and medical information.

In conjunction and collaboration with the third-party review team, Ibex continued to diligently review and reconcile the information with internal and public records in furtherance of identifying the individuals to whom the data relates and the appropriate contact information for those individuals. These efforts were

completed on or around July 11, 2021, at which time Ibex determined the scope of impacted individuals and the types of protected data associated with those individuals.

Ibex thereafter worked to provide notification to potentially impacted individuals as quickly as possible. Importantly, there is no indication that individuals' specific information was accessed or misused. However, Ibex is notifying all potentially impacted individuals out of an abundance of caution.

Notice to New Hampshire Residents

On or about August 6, 2021, Ibex provided written notice of this incident to all affected individuals, which includes fifty-six (56) 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, Ibex moved quickly to investigate and respond to the incident, assess the security of Ibex systems, and notify potentially affected individuals. Ibex has implemented additional cybersecurity measures to further protect against similar incidents moving forward. Ibex is also providing access to credit monitoring services for twelve (12) months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ibex 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. Ibex 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) 930-1509.

Very truly yours,

Gregory Bautista of
MULLEN COUGHLIN LLC

GJB:rrg
Enclosure

Exhibit A

ibex.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data <<Variable Header>>

Dear <<Name 1>>:

Ibex Global Solutions, Inc. ("Ibex") writes to make you aware of an incident that potentially affects the security of your information. This letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On August 17, 2020, Ibex learned that it was the victim of a malware attack that impacted the availability of a limited segment of our systems. We immediately took these systems offline and, with the assistance of third-party computer specialists, launched an investigation to determine the nature and scope of the incident. On or about September 15, 2020, the investigation confirmed that certain files on our systems may have been accessed without authorization between July 27 and August 17, 2020. We therefore undertook a meticulous and time-intensive review of the potentially impacted files and our internal systems in order to identify the information that was involved and to whom it related. In connection with this review, on or about September 29, 2020, a third-party firm was engaged to review the potentially impacted files. Ibex, upon receiving and validating the findings of the third-party firm, on or about June 14, 2021, determined that one or more of the potentially impacted folders included information related to individuals.

In conjunction and collaboration with the third-party review team, Ibex continued to diligently review and reconcile the information with internal and public records in furtherance of identifying the individuals to whom the data relates and the appropriate contact information for those individuals. These efforts were completed on or around July 11, 2021, at which time Ibex determined the scope of impacted individuals and the types of protected data associated with those individuals.

We thereafter worked to provide notification to potentially impacted individuals as quickly as possible. **Importantly, there is no indication that your specific information was accessed or misused. However, we are notifying potentially impacted individuals out of an abundance of caution.**

What information was involved? Our investigation determined that the information related to you that may have been potentially affected includes your name, <<Breached Elements>>.

What we are doing? Information security is among Ibex's highest priorities, and we have strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We have implemented additional cybersecurity measures to further protect against similar incidents moving forward. We reported this incident to law enforcement and are cooperating with their investigation. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information.

As an added precaution, we are also offering <<Variable Data>> months of complimentary access to credit monitoring, fraud consultation, and identity theft restoration services through Equifax. Individuals who wish to receive these services must enroll by following the enrollment instructions found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*.

What can you do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to protect your information in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 866-871-8614 Monday through Friday from 9 am to 9 pm Eastern Time.

We take this incident very seriously and sincerely regret any inconvenience or concern this incident caused you.

Sincerely,

James D. Ferrato
Chief Information Officer
Ibex Global Solutions, Inc.
(Enclosure)

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in credit monitoring through Equifax.

EQUIFAX®

Enter your Activation Code: *<<Activation Code>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold
*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of *<<Activation Code>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To sign up for US Mail delivery, dial 1-855-833-9162 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.
1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Monitor 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	1-888-397-3742	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: 441 4th St. NW #1100 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. Leaders Life is located at 1350 South Boulder Avenue W #900 Tulsa, Oklahoma 74119.

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 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, 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/.

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 approximately [#] Rhode Island residents impacted by this incident.