Proskauer Rose LLP 1001 Pennsylvania Avenue, NW Suite 600 South Washington, DC 20004-2533

RECEIVED
FEB 15 2022
CONSUMER PROTECTION

Ryan P. Blaney
Member of the Firm
d 202.416.6815
f 202.416.6899
RBlaney@proskauer.com
www.proskauer.com

February 11, 2022

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

Dear Attorney General Formella:

I am writing to you on behalf of my client, Component Assembly Systems, Inc. ("CAS"), a New York corporation with offices at 620 Fifth Avenue, Pelham, NY 10803 and the Federal Employer Identification Number (FEIN) of 11-6033867, to notify you of a recent cybersecurity incident, pursuant to New Hampshire's breach notification law. In total, 170 individuals were affected, including three residents of New Hampshire.

Around November 2, 2021, malicious actors gained access to Component Assembly Systems, Inc. computer systems in a "ransomware"-type extortion attempt. Discovered within a few hours, the CAS team shutdown all systems and network communications. CAS then hired third-party digital forensics investigators to review the event in order to know whether any unencrypted data was taken by the attackers. Review by the forensics investigators concluded on January 12, 2022 and revealed that user account names and password hash had likely been downloaded. The malicious actors then used the stolen user credentials to compromise a number of email accounts and download their contents. CAS did not communicate with the attackers, nor pay any ransom.

In depth review of the data, which concluded in mid-January, determined that there were emails containing job application information exposed to the attackers. The data accessed included new-hire paperwork, accident reports and change of address forms, Social Security Numbers, driver's licenses and passports.

CAS took many steps throughout to confirm the security of its systems, taking prudent steps such as forcing password changes for all employees. CAS then implemented increased security measures, conducted additional employee training, and are currently reviewing and implementing changes to our policies and procedures relating to employee information. CAS is notifying all affected individuals, and is exceeding its legal obligation by offering 24-months of free credit monitoring services to all affected individuals.

CAS and the investigators were unable to identify the attackers. There has been no evidence uncovered of actual or attempted misuse of the information taken in this attack. No report has been made to law enforcement, except where required by state law.

CAS has a number of safeguards in place to further protect against this kind of attack, including a written information security program. CAS is also reviewing its security policies and procedures to enhance how it protects these systems. CAS began notifying New Hampshire residents on February 11, 2022 via U.S.

Mail, with information on how the individual may access the free credit monitoring. A de-identified copy of the letter that is being sent to the affected individuals is enclosed herein.

If your office requires any further information in this matter, please contact me at (202) 416-6815 or rblaney@proskauer.com.

Sincerely,

Ryan P. Blaney

Enclosure

EXHIBIT A

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

February 11, 2022

Re: Notice of Data Incident

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

Component Assembly Systems, Inc. ("CAS", "us", "we") is writing to notify you of a recent incident that may have affected the privacy and security of some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information about the incident, our response to it, and information related to what you may do to better protect your personal information, should you feel it appropriate to do so.

What Happened? In November 2021, malicious actors gained access to CAS computer systems in an extortion attempt. Discovered within a few hours, our team shut down all systems and network communications. We hired third-party experts to review the event in order to know whether any unencrypted data was taken by the intruders. Review by Forensics Investigators concluded on January 12, 2022 and revealed that user account names and password hash had likely been downloaded. The malicious actors then used the stolen user credentials to compromise a number of email accounts and download their contents. In depth review of the data, which concluded in mid-January, determined that there were emails containing job application information.

What Information was Involved? The data accessed included new hire paperwork, accident reports and change of address forms, containing Social Security Numbers, driver's licenses and passports.

What Are We Doing? Information, privacy, and security are among our highest priorities. CAS has strict security measures in place to protect the information in our care. Upon learning of this incident, we quickly took steps to investigate and confirm the security of our systems, and in an abundance of caution, we forced password changes for all employees. As part of our ongoing commitment to the security of information, we implemented increased security measures, conducted additional employee training, and are currently reviewing and implementing changes to our policies and procedures relating to employee paperwork. Additionally, we are also providing all required regulatory notices. This notice was not delayed as a result of a law enforcement investigation.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We have secured the services of NortonLifeLock, Inc. to provide identity and credit monitoring services at no cost to you for twenty-four (24) months. For more information on these services, please review the enclosed "Steps You Can Take to Protect Your Information."

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also enroll in LifeLock Defender Preferred to receive the identity and credit monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

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 call center at (866) 918-4179 (toll-free), available 24/7. You may also contact Component Assembly Systems, Inc. by writing to us at 620 Fifth Avenue, Pelham, NY 10803, Attn: Human Resources.

Component Assembly Systems takes the privacy and security of the personal information in our care seriously. Please let us know if you have any questions.

Sincerely,

Steps you can take to protect your information
Complimentary Credit Monitoring and Identity Protection Services

Component Assembly Systems, Inc. has retained NortonLifeLock, Inc. to provide twenty-four (24) months of complimentary LifeLock Defender™ Preferred identity theft protection.

I. To activate your membership online and get protection at no cost to you:

1. In your web browser Click on the yellow "START MEMBERSHIP" button (do not attempt registration from a link presented by a search engine).
2. You will be taken to another page where, below the THREE protection plan boxes, you may enter the and click the "APPLY" button.
3. On the next screen, enter your nd click the "APPLY" button.
4. Your complimentary offer is presented. Click the red "START YOUR MEMBERSHIP" button.
5. Once enrollment is completed, you will receive a confirmation email (be sure to follow ALL directions in this email).

II. Alternatively, to activate your membership over the phone, please call:

III. **You will have until May 31, 2022 to enroll in this service.**

Once you have completed the LifeLock enrollment process, the service will be in effect. Your LifeLock Defender™ Preferred membership includes:

- ✓ Primary Identity Alert System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ Norton™ Security Deluxe[2] (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to $25,000†††
- ✓ Personal Expense Compensation up to $25,000†††
- ✓ Coverage for Lawyers and Experts up to $1 million†††
- ✓ U.S-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores[1]**
  The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring[1]**
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts†**

[1]If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
[2] Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.
**These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Defender Preferred. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order 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, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

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 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.