

RECEIVED

100 International Drive
23rd Floor
Baltimore, MD 21202

MAY 28 2022

P 1.248.646.5070
F 1.248.646.5075

CONSUMER PROTECTION

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

May 18, 2022

Privileged and Confidential
VIA EMAIL AND FIRST-CLASS MAIL

Hon. John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301
attorneygeneral@doj.nh.gov

Re: Security Breach Notification

Dear Attorney General Formella:

We are writing on behalf of our client, Clements Worldwide Insurance (“Clements Worldwide”) (located at 1301 K Street NW, Suite 1200 West, Washington, DC 20005), to notify you of a data security incident involving one (1) New Hampshire resident.¹

Nature

On October 28, 2021, Clements Worldwide discovered that it was the victim of a ransomware incident that impacted its networks and servers. After discovering the incident, Clements Worldwide took steps to secure and safely restore its systems. Further, Clements Worldwide engaged our firm and third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and to assist in the remediation efforts. On January 20, 2022, Clements Worldwide concluded its initial investigation and determined that the unauthorized individual likely gained access to its systems via a vulnerability found in the environment of one of its vendors.

Clements Worldwide performed a comprehensive review of the compromised data to determine the types of protected information exposed and to identify individuals potentially impacted by the incident. On February 18, 2022, Clements Worldwide concluded its initial review and determined that the incident potentially involved one (1) New Hampshire resident. Further, on May 16, 2022, Clements Worldwide located the most recent contact information for these individual(s).

¹ By providing this notice, Clements Worldwide 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.

The personal information obtained potentially included name, date of birth, driver's license number, passport number, and social security number.

Notice and Clements Worldwide's Response to the Event

On May 18, 2022, Clements Worldwide mailed a written notification pursuant to N.H. Rev. Stat § 359-C:19, in a substantially similar form as the enclosed letters (attached as Exhibit A).

Further, Clements Worldwide is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through TransUnion;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- 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 and law enforcement to report attempted or actual identity theft and fraud.

Further, Clements Worldwide provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary). Finally, Clements Worldwide is working to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

Clements Worldwide
P.O. Box 3923
Syracuse, NY 13220



1301 K STREET NW, SUITE 1200 WEST
WASHINGTON, DC 20 005 USA
P. +1.202.872.0060
800.872.0067
F. +1. 202.466.9064
E. info@clements.com

CLEMENTS.COM

XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

May 18, 2022

Re: Notice of Data Breach

Dear XXXXXXXXXXXX,

At Clements Worldwide, we value transparency and respect the privacy of your information. We are contacting you today, as precautionary measure, to let you know about a data security incident that impacted part of our systems at the end of last year and may have impacted some of your personal data. This letter contains important information about what personal data was potentially impacted, what this means for you, the support we are offering, and the steps we have taken since to further enhance our security systems.

What Happened

On October 28, 2021, we discovered suspicious activity that affected our networks and servers. This was caused by an IT security incident that resulted in unauthorized temporary access to our systems.

After discovering the incident, we quickly took steps to secure and safely restore our systems and operations. Further, we engaged outside counsel and third-party forensic experts to assist in the remediation efforts and conduct a thorough investigation of the incident's nature and scope. We also contacted the FBI to seek assistance and guidance, as one of the many organizations confronting the impacts of the evolving cyber threat landscape. Based on the results of our investigation, we were able to determine that a data breach likely occurred on October 7, 2021.

We have now concluded our investigation, which found evidence to suggest that an unauthorized party was able to access data. Part of our investigation focused on assessing exactly what data was accessed, but unfortunately, this is a complex process, and the forensic analysis could not definitively determine the specific records or data that may have been accessed or obtained. As such, and out of an abundance of caution, we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information. *However, we currently have no evidence indicating that any information has been used for identity theft or financial fraud.*

What Information Was Involved

The types of information potentially involved (only if you provided us this information) are your name, date of birth, driver's license number, passport number, and social security number. *However, as stated above, we currently have no evidence indicating that any information has been used for identity theft or financial fraud.*

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. As explained above, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

As stated above, while we have no evidence indicating that your information has been used for identity theft or fraud, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. In addition, please see "**OTHER IMPORTANT INFORMATION**" on the following pages for guidance on how to best protect your identity.

Finally, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: **XXXXXXXXXX**.

In order for you to receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, please contact me at [REDACTED]

Sincerely yours,

Adam Steward, Compliance Manager

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax (888) 766-0008 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	Experian (888) 397-3742 P.O. Box 2104 Allen, TX 75013 www.experian.com	TransUnion (800) 680-7289 P.O. Box 1000 Chester, PA 19016 www.transunion.com
--	---	---

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below).

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	TransUnion Security Freeze & Fraud Victim Assistance Dept. P.O. Box 380 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze
---	---	---

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC

will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.consumer.ftc.gov/identity-theft) or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/>.

District of Columbia residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov. **Iowa residents** may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa*, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents:** State law advises you that you have the right to obtain a police report. Further, you have the right to obtain a security freeze on your credit report free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. To request a security freeze be placed on your credit report, please be prepared to provide any or all of the following: your full name, social security number, address(es), date of birth, a copy of a government issued identification card, a copy of a utility bill, bank or insurance information, or anything else the credit reporting agency needs to place the security freeze. Further information regarding credit freezes, including the contact information for the credit reporting agencies, may be found above in section titled "Security Freeze (also known as a Credit Freeze)." **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **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. **New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: New York Attorney General's Office Bureau of Internet and Technology, (212) 416-8433, <https://ag.ny.gov/internet/resource-center> and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, <https://www.dos.ny.gov/consumerprotection>. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division*, 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents:** State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting

agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.