Baker McKenzie LLP
300 East Randolph St.
Ste. 5000
Chicago, IL 60601
United States
Tel: +1 312.861.8000
www.bakermckenzie.com

July 20, 2023

VIA EMAIL
New Hampshire Attorney General
attorneygeneral@doj.nh.gov

RE: Data Breach Reporting

Dear New Hampshire Attorney General:

I am writing on behalf of Quinn Emanuel Urquhart & Sullivan, LLP ("QEUS") to notify you of a data security incident. Specifically, a data center used by a vendor of QEUS suffered a ransomware incident. QEUS was notified on or about May 16, 2022 that its vendor had suffered a ransomware attack on or about May 14, 2022. In response to this incident, QEUS engaged a leading third-party cybersecurity forensics firm to determine the scope of the incident. In the course of the investigation, QEUS determined that a limited number of files hosted by the data center may have been subject to unauthorized access and acquisition. This incident did not involve unauthorized access to any QEUS systems.

QEUS is taking steps to protect the affected individuals following this incident. Following a thorough investigation with the assistance of its third-party partners, QEUS confirmed that personal information relating to approximately 1,974 individuals was included in the files that may have been subject to unauthorized access and acquisition, approximately 5 of which are New Hampshire residents. The potentially-impacted personal information for some individuals included

.

QEUS is providing notice to all potentially-affected individuals. Notice to these individuals who are residents of New Hampshire will be sent on or about July 20, 2023 by postal mail. A copy of this notice is attached. These individuals are also being provided of credit monitoring services through Experian, at no cost to them.

Please feel free to contact me with any questions at
or .

Regards,

Brian Hengesbaugh
Partner

Quinn Emanuel Urquhart & Sullivan, LLP
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 20, 2023

[redacted]

RE: Notice of Data Breach

[redacted]

Quinn Emanuel Urquhart & Sullivan, LLP ("QEUS") is writing to inform you of a data security incident that may have impacted some of your personal information. You may not have heard of QEUS, but we provide professional legal services to clients in a wide variety of industries and business sectors. In order to serve our clients, we collect relevant data from our clients and opposing parties. We want to provide you with details regarding the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What happened?

On or around May 14, 2022, an electronic discovery vendor that collects and processes QEUS's electronic discovery data suffered a cybersecurity incident. Upon becoming aware of the incident, QEUS began coordinating with the data center and vendor to better understand the scope and impact of the incident. QEUS proceeded to engage third-party cybersecurity experts to remediate, further investigate what happened, and determine the scope of the incident. Our investigation determined that an unknown party accessed or acquired data within certain segments of the data center's network between May 13, 2022 and May 14, 2022.

What information was involved?

The impacted personal information relating to you includes your [redacted]

What are we doing?

The privacy and security of information entrusted to QEUS is of the utmost priority. Upon learning of the incident, QEUS took steps with its vendors to further protect the privacy and security of the data entrusted to them. We also reported this incident to law enforcement.

[redacted]

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. We recommend you review the information contained in the attached "Steps You Can Take to Help Protect Your Information."

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for through Experian at no cost to you. If you wish to activate these services, you may follow the instructions included below. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by . Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

[redacted]

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For more information.

If you have additional questions, please call [redacted], Monday through Friday, 8:00 a.m. to 10:00 p.m., Central and Saturday, and Sunday, 10:00 a.m. to 7:00 p.m., Central, (excluding major U.S. holidays).

We sincerely regret any inconvenience this incident may cause you. Protecting information entrusted to QEUS and its vendors is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Quinn Emanuel Urquhart & Sullivan, LLP

*Offline members will be eligible to call for additional reports quarterly after enrolling.

**The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

[redacted]

Steps You Can Take to Help Protect Your Information

- You may wish to visit the website of the U.S. Federal Trade Commission at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
- You may have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.
- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: *(1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint*. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.
    - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
    - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
    - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000
- For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
- For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566- 7226.
- For New York residents: You may contact the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.
- For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at (401) 274- 4400, https://riag.ri.gov/about-our-office/contact-us. The number of affected Rhode Island residents is six (6).
- For the District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://oag.dc.gov/about-oag/contactus.
- 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and (vi) 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_ your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.