MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 29, 2019

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

We represent Aquiline Holdings, LLC and its affiliate Aquiline Capital Partners, LLC (collectively, "Aquiline"), with a primary office at 535 Madison Avenue, New York, New York 10022. We write to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. By providing this notice, Aquiline 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 January 28, 2019 Aquiline identified an unauthorized login into an employee's email account by someone who had set up specific mail rules to auto-forward emails containing certain key words. Upon identifying this unauthorized access, Aquiline immediately shut down the mailbox and, in consultation with external cyber security experts, conducted a comprehensive investigation into the incident which determined that the Aquiline employee's email account was accessed without authorization on January 28, 2019. This investigation also confirmed that none of the auto-forwarded emails contained any personal information.

However, because the email account was subject to unauthorized access and Aquiline was unable to confirm what, if any, emails and attachments were viewed, Aquiline undertook a thorough analysis of all messages and documents contained in the mailbox at the time of the incident to determine whether they contained any protected information. Aquiline received an initial data file of potentially impacted individuals on May 10, 2019. However, this data file lacked complete address information related to individuals, and required additional internal work to de-duplicate, reformat, and update. Aquiline then took steps to confirm address information for the potentially impacted individuals for purposes of providing notification to those individuals and completing the required de-duplication. Aquiline confirmed the impacted email accounts

contained personal information relating to one (1) New Hampshire resident including: name, Social Security number, and financial account information.

Notice to New Hampshire Resident

On October 29, 2019, Aquiline provided written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. 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, Aquiline moved quickly to investigate and respond to the incident, assess the security of Aquiline's systems and notify potentially affected individuals. Aquiline has strict security measures in place to protect information and upon learning of this incident, took additional steps relating to its employee email accounts. Aquiline reset passwords for Aquiline email accounts and is reviewing policies and procedures relating to data security.

Aquiline is also providing access to identity and credit monitoring services for 12 months, through Experian, to individuals whose personal information was potentially accessible during the period of unauthorized access, at no cost to these individuals.

Additionally, Aquiline 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. Aquiline 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. Aquiline is also providing relevant regulatory notifications.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin of
MULLEN COUGHLIN LLC

PTM/plm
Enclosure

EXHIBIT A

Aquiline Capital Partners LLC
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

AQUILINE
CAPITAL PARTNERS LLC

October 29, 2019

[redacted]

Dear [redacted],

We are writing to notify you of a cyber security incident at Aquiline Capital Partners LLC (Aquiline).

What Happened?
On January 28, 2019 Aquiline identified an unauthorized login into an employee's email account by someone who had set up specific mail rules to auto-forward emails containing certain key words. Upon identifying this unauthorized access, Aquiline immediately shut down the mailbox and, in consultation with external cyber security experts, conducted a comprehensive investigation into the incident which determined that, while 50 emails had been forwarded, none of those emails contained social security numbers, account numbers, or any other Personal Identifying Information ("PII"). This forensic investigation included a thorough analysis of all messages and documents contained in the mailbox at the time of the incident. Even though none of your PII was in the emails forwarded outside of the impacted email account, we are notifying you in an abundance of caution because some of your PII was present in other (non-forwarded) emails contained in this email account.

What Information Was Involved?
Aquiline's investigation could not confirm what information, if any, was actually viewed by the unauthorized individual(s). However, we were able to determine that only 50 emails had been forwarded from the impacted email account and that none of those forwarded emails contained PII. Additionally, we confirmed that no other documents or applications on Aquiline servers were accessed.

What We Are Doing?
Aquiline is committed to information privacy and cybersecurity. Aquiline has long had comprehensive security measures in place to protect information in our care. Upon learning of this incident, Aquiline took several additional measures to further enhance the security of our systems, including employee email accounts. Aquiline regularly assesses our policies and procedures relating to data security to ensure that we maintain sufficient cybersecurity protection.

What Can You Do?
Please review the information contained in the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud". Additionally, we have engaged the services of Experian to provide identity and credit monitoring services at no cost to you for 12 months, further information of which can be found herein. For further information about this service, please call 877-288-8057.

For More Information.
We understand that you may have additional questions about this incident. Please contact Geoff Kalish at gkalish@aquiline.com or (212) 624-9535 or Ezra Berger at eberger@aquiline.com or (212) 624-9511 with any questions or concerns.

Aquiline takes the privacy and security of the personal information in our care very seriously. We sincerely regret this incident.

Sincerely,

Jeff Greenberg
Chairman
Aquiline Capital Partners

Steps You Can Take to Protect Against Identity Theft and Fraud

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: 12/31/2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057 by **12/31/2019.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

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 agents 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-288-8057. 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 (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).

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

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**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more 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.

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, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.