



MULLEN  
COUGHLIN<sup>LLC</sup>

RECEIVED

NOV 19 2018

CONSUMER PROTECTION

Jennifer A. Coughlin  
Office: 267-930-4774  
Fax: 267-930-4771  
Email: jcoughlin@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

November 16, 2018

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Valor Management Corp. (“Valor”), 875 N. Michigan Avenue, Suite 3214, Chicago, IL 60611, and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Valor does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

**Nature of the Data Event**

On or about October 16, 2018, Valor learned of suspicious activity occurring within certain employee email accounts. Valor immediately took steps to secure the email accounts and worked with third-party forensic experts to determine the nature and scope of the incident. On or around November 7, 2018, the investigation confirmed that two email accounts may have been accessible to an unauthorized actor through the compromise of email account credentials. Valor reviewed the impacted accounts to confirm the information potentially accessible to the unauthorized actor, and the identities of the impacted individuals.

The personal information impacted by this event may include the following: name, address, tax identification number, and account balance. A small number of individuals may also have had passport and/or driver’s license information and bank account information impacted. To date, Valor has not received any reports of the misuse of this information.

**Notice to New Hampshire Resident**

On November 16, 2018, Valor began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

**Other Steps Taken and To Be Taken**

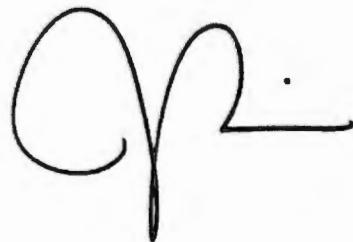
Upon discovering the potential unauthorized access to the email accounts, Valor moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. Valor is also working to implement additional safeguards to protect the security of information in its system.

Valor is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to two (2) years of credit and identity monitoring services, including identity restoration services through TransUnion, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Valor is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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. Valor is also providing written notice of this incident to other state regulators, as necessary.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4774.

Very truly yours,

A handwritten signature in black ink, appearing to read "J. Coughlin".

Jennifer Coughlin of  
MULLEN COUGHLIN LLC

# **EXHIBIT A**



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>>

Dear <<Name 1>>:

**Re: Notice of Data Breach**

Valor Management Corp. (“Valor”) is writing to inform you of a recent event that may impact the privacy of some of your personal information. You are being provided with this letter because of your association with <<Entity Name>>. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On or about October 16, 2018, Valor learned of suspicious activity occurring within certain employee email accounts. We immediately took steps to secure the email accounts and worked with third-party forensic experts to determine the nature and scope of the incident. On or around November 7, 2018, the investigation confirmed that two email accounts may have been accessible to an unauthorized actor through the compromise of email account credentials. We conducted an extensive review of the impacted accounts to confirm the information potentially accessible to the unauthorized actor, and the identities of the impacted individuals.

**What Information Was Involved?** A review of the impacted email accounts determined that the following types of information related to you may have been accessible: your name, address, tax identification number, and account balance. A small number of individuals may also have had passport and/or driver’s license information and bank account information impacted. Your tax identification number may also be your Social Security number. To date, we have not received any reports of the misuse of your information.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately secured the affected email accounts. While we have procedures in place whereby information additional to that contained in the email accounts is needed in order to conduct any investment activity, as part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our existing policies and procedures and implementing additional safeguards to further secure the information in our systems. We also notified state regulators, as required. As an added precaution, we are also offering you complimentary access to 2 years of credit monitoring services.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Better Protect Your Information*. There, you will also find more information on the credit monitoring services we are offering and how to enroll. We also recommend you confirm the accuracy of any communication instructing you to send money to a bank account.

**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 888-510-9594 between 8:00 a.m. and 8:00 p.m. Central Time, Monday through Friday. You may also write to Valor at 875 N. Michigan Avenue, Suite 3214, Chicago, IL 60611.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Antonio J. Gracias  
President and CEO

## **STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at [www.mytrueidentity.com](http://www.mytrueidentity.com) and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<Insert Unique 12- letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian, and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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](http://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**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://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:

<b>Experian</b> P.O. Box 2002 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud:center.html">www.experian.com/fraud:center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19106 1-800-680-7289 <a href="http://www.transunion.com/fraud-victim-resource/place-fraud-alert">www.transunion.com/fraud-victim-resource/place-fraud-alert</a>	<b>Equifax</b> P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	---	--

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](http://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](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

To monitor for actual or attempted misuse of Social Security benefits, you can create an account at <https://www.socialsecurity.gov/myaccount>. If you see an error or attempted misuse of social security benefits, you can go to your local Social Security Office for assistance. Local offices can be found using the following office locator - <https://secure.ssa.gov/ICON/main.jsp>.

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](http://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.