



RECEIVED

SEP 30 2021

September 27, 2021

CONSUMER PROTECTION
Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Certified Mail; Return Receipt Requested

Attorney General John Formella
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Cybersecurity Incident Involving Aladdin Capital

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Aladdin Capital (“AC”), a commercial equipment leasing firm, located at 1201 W Russell St, Sioux Falls, South Dakota, with respect to a recent cybersecurity incident that was first discovered by AC on November, 24th, 2020 (hereinafter, the “Incident”). AC takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that AC has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On or around November 24th, 2020, AC became aware of suspicious activity related to some of AC employee’s email account when they found evidence of fraudulent emails being sent from these accounts. Upon discovery of this incident, AC, with the assistance of a specialized cybersecurity firm, conducted a forensic investigation to determine the full nature and scope of this incident by analyzing every AC mailbox and system to ensure the unauthorized individual was no longer present within the environment, and to identify which accounts and systems may have been impacted as a result of this unauthorized access. The investigation took a considerable amount of time, but AC was able to conclude that unauthorized access may have occurred to the contents of only two of the email accounts between November 18, 2020 and November, 23, 2020. Based on these findings, AC looked into data mining options to identify the exact individuals whose sensitive personal information was stored within these accounts. However, in order to avoid delaying notification any longer, out of an abundance of caution, AC proceeded to notify all of its clients and potential clients whose personal information may have been stored in the two compromised email accounts.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com



Although AC is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, driver's license or state identification number, Social Security number, date of birth, financial information, electronic signature, and the associated business's tax identification number may have been exposed as a result of this unauthorized activity.

As of this writing, AC has not received any reports of related identity theft since the date of the Incident November, 24th 2020 to present.

2. Number of New Hampshire residents affected.

AC identified and notified 2318 individuals potentially affected by this Incident. Of those, one (1) was a resident of New Hampshire. Notification letter to this individual was mailed on September 27, 2021, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

AC is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, AC moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, AC engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, they reset all user passwords, implemented two-factor authentication, revised the policies and procedures on business email practices, re-trained employees on data security, amended the administrative, technical, and physical safeguards, and removed personal information from the email servers. Lastly, AC informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although AC is not aware of any actual or attempted misuse of the affected personal information, AC offered 12 months of complimentary credit monitoring and identity theft restoration services through TransUnion to all individuals to help protect their identity. Additionally, AC provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

AC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.



Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in black ink, appearing to read "Anjali C. Das". The signature is fluid and cursive.

Anjali C. Das

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>>

Via First-Class Mail

<<Date>>

Re: Notice of data breach

Dear <<Name 1>>,

Aladdin Capital (“AC”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access of your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the misuse of your information.

What Happened?

On or around November 24th, 2020, AC became aware of suspicious activity related to some of AC’s employees’ email accounts when they found evidence of fraudulent emails being sent from these accounts. Upon discovery of this incident, AC, with the assistance of a specialized cybersecurity firm, conducted a forensic investigation to determine the full nature and scope of this incident by analyzing every AC mailbox and system to ensure the unauthorized individual was no longer present within the environment, and to identify which accounts and systems may have been impacted as a result of this unauthorized access. The investigation took a considerable amount of time, but AC was able to conclude that unauthorized access may have occurred to the contents of only two of the email accounts. Based on these findings, AC looked into data mining options to identify the exact individuals whose sensitive personal information was stored within these accounts. However, in order to avoid delaying notification any longer, out of an abundance of caution, AC proceeded to notify all of its clients and potential clients whose personal information may have been stored in the two compromised email accounts.

What Information Was Involved?

Again, not every individual was impacted by this incident and AC is providing this notice out of an abundance of caution. However, the information that may have been subject to unauthorized access included your name, address, driver’s license or state identification number, Social Security Number, date of birth, financial information, electronic signature, and your business’s tax identification number.

What We Are Doing

We are committed to doing everything we can to help protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken and will continue to take steps to mitigate the risk of future issues. Specifically, we have reset all user passwords, implemented two-factor authentication, revised our policies and procedures, re-trained our employees on data security, amended our administrative, technical, and physical safeguards, and removed personal information from our email servers.

Out of an abundance of caution, we are also providing you with 12 months of complimentary credit monitoring services through TransUnion. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can 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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the credit monitoring services we are making available to you.

To enroll in this service, go directly to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code << 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, 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 << Engagement Number >> 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.

Once you are enrolled, you will be able to obtain 12 Months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provide assistance in the event 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.)

You can sign up for the myTrueIdentity online Credit Monitoring service anytime between now and << Enrollment Deadline >>. 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 credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your myTrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

Again, we are making these services available to you at no cost; however, you will need to activate yourself in these services. The deadline to enroll is << Enrollment Deadline >>.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 877-869-9023 (toll free) during the hours of 9 a.m. and 9 p.m. Eastern Standard Time, Monday through Friday (excluding U.S. national holidays).

AC sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



Scott Keogh
Vice President
Aladdin Capital

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-alerts

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 at 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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov
