

October 29, 2021

James A. Paulick
Jpaulick@leechtishman.com
Direct Dial: (213) 246-4967

Via Certified Mail

Office of Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Data Incident

Dear Sir or Madam:

We represent Managed Markets Insight & Technology, LLC's (MMIT). MMIT is a company that provides customers with market access data, analytics and insights to a team of pharmacists, clinicians, data specialists and market researchers. MMIT is located at 1040 Stony Hill Road, #300 Yardley, PA 19067.

We are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MMIT 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 Wednesday afternoon, October 6, 2021, at 12:55 p.m. EDT, an MMIT employee unknowingly fell victim to a phishing attempt. The attacker sent a phishing email with a message stating that her email was full and provided a link that directed her to a malicious site where she submitted her Microsoft O365 credentials. It was not until the next day, Thursday evening, October 7, 2021, at 4:54 p.m. EDT that MMIT was alerted from its SOC provider, AWN (Arctic Wolf Networks) that her credentials were compromised. The compromised account was locked down and disabled within minutes by the MMIT NetOps team. At this point, the incident was contained, and an incident response investigation was launched to determine the scope and severity of the attack.

On Friday morning, October 8, 2021, at 8:40 a.m. EDT, the MMIT NetOps team determined that the attackers had brief access to an excel spreadsheet containing personally identifiable information. The categories of the personal

information subject to the breach are as follows: full names, mailing addresses, social security numbers, and email addresses. There were no other alerts that any other information had been viewed or exfiltrated. After MMIT NetOps and Information Security teams finished conducting the investigation, it was concluded that the attackers were only able to gain "View-Only" access, and no sensitive data of any MMIT Vendor was exfiltrated (e.g., downloaded, extruded, or exported) besides what the attacker was able to capture while "viewing" the compromised file.

NOTICE TO NEW HAMPSHIRE RESIDENT

MMIT's investigation to date has revealed that one (1) New Hampshire resident's personal identifiable information may have been compromised in the data breach. Written notice will be provided in substantially the same form as the template letter attached here as *Exhibit A*. We estimate the letter to the New Hampshire resident will be mailed by Wednesday November 3, 2021. MMIT is providing credit monitoring services for twenty-four (24) months, through Kroll LLC, at no cost to this individual.

OTHER STEPS TAKEN AND PLAN TO BE TAKEN

MMIT moved quickly to investigate and respond to the incident, assess the security of MMIT systems, and notify potentially affected individuals. MMIT diligently informed law enforcement by October 9, 2021. MMIT is also working to implement additional safeguards and training to its employees. As mentioned above, MMIT is providing access to credit monitoring services for twenty-four (24) months, through Kroll LLC, at no cost to this individual.

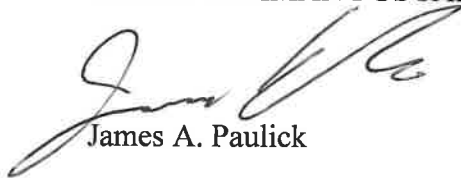
Additionally, MMIT is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. MMIT is providing individuals with information 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.

CONTACT INFORMATION

Should you have any questions regarding this notification or other aspects of the data security incident, please contact Jim Paulick, from Leech Tishman, at 213-246-4967.

Very truly yours,

LEECH TISHMAN FUSCALDO & LAMPL, LLC

A handwritten signature in dark ink, appearing to read "Jim Paulick", is written over the printed name.

James A. Paulick

Enclosure: Exhibit A: Notice to Individuals



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

As a precautionary measure, we are providing notice of a data breach which involves MMIT Vendor Information (as defined below) relating to certain vendors of the MMIT group of companies (including Managed Markets Insight and Technology, RJ Health International, The Zitter Group, the Dedham Group, and Pulse Analytics) ("MMIT Vendors").

What Happened?

MMIT conducted a thorough investigation of a data breach which included MMIT Vendor Information which occurred on October 7, 2021. The investigation revealed that certain MMIT Vendor Information was potentially in view but no sensitive data of any MMIT Vendor was downloaded.

MMIT Vendor Information

The potentially viewed data included vendor information, such as individual names, employer identification and Social Security numbers, business and personal addresses, and email addresses ("MMIT Vendor Information").

What Are We Doing?

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(Activation Deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing your services is included with this letter.

For More Information

If you have questions, please call 1-??-??-???, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Remain Vigilant: As always, you should monitor your statements for any activity you do not recognize. Contact local law enforcement and credit monitoring agencies and consumer affairs agencies immediately to report any suspicious activity.

Ordering Your Free Credit Report: You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. You may also obtain information from these sources about fraud alerts and security freezes. To order your credit report, visit www.annualcreditreport.com or call toll-free at 877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

Additional Contact Information

US Attorney General U.S.
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
800-877-8339
<https://www.justice.gov/contact-us>

Experian Inc.
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

TransUnion LLC
P.O. Box 2000
Chester, PA 19022-2000
888-909-8872
www.transunion.com

Equifax Credit Information
Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
800-685-1111
www.equifax.com



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.