pillsbury

Pillsbury Winthrop Shaw Pittman LLP
725 South Figueroa Street, 36th Floor | Los Angeles, CA 90017-5524 | tel 213.488.7100 | fax 213.629.1033

Catherine D. Meyer
tel: 213-488-7236

October 19, 2022

Office of the Attorney General
Department of Justice
Consumer Protection Bureau
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: **Notification of Data Security Incident**

Dear Sir/Madam:

This letter is being sent in accordance with state law to inform your office that the name and credit card information of one New Hampshire resident may have been subject to unauthorized access.

We represent WM Symposia, Inc., PO Box 27646, Tempe AZ 85285-7646, in connection with a potential data breach incident which occurred when WM Symposia's service provider, X-CD discovered malicious code on the event registration platform service it provided to our client. X-CD advised WM Symposia that unauthorized third parties placed malware on X-CD's system which may have allowed access to the name and credit card data by unauthorized person(s). WM Symposia does not collect, store, or process credit card information; all transactions are processed by X-CD. WM Symposia does not have information that the individual data was actually accessed or has been misused but, in an abundance of caution, is notifying the individuals who accessed the X-CD registration platform during the period when the malware was present (January 1, 2022 through April 20, 2022) of the incident.

We have enclosed a copy of the notice letter that is being mailed to affected individuals on or about October 17, 2022. Notification has been delayed because the report from X-CD was only recently received by WM Symposia.

The three Consumer Reporting Agencies have not been notified of this incident. Upon learning of this potential incident WM Symposia has:

- Required and confirmed that X-CD discontinue use of its previous payment processing module and instituted use of Authorize.net for processing of credit card payments; this prevents X-CD access to any credit card information
- Required X-CD to conduct a full forensic review to identify the cause and scope of the incident
- Received assurance from X-CD that they have successfully removed the malicious code from their software
- Hired a cybersecurity subject matter expert to (a) evaluate and update WM Symposia security procedures and (b) evaluate the X-CD conference platform
- Updated all passwords and VPN access for all WM Symposia personnel
- Conducted a vulnerability assessment for WM Symposia personnel computers and systems
- Hired a Chief Information Security Officer (CISO) to evaluate the WM Symposia systems for security issues on a regular basis

Should you have any additional questions, you may contact me directly at (213) 488-7362.

Very truly yours,

Catherine D. Meyer
Senior Counsel

WM SYMPOSIA EDUCATION & OPPORTUNITY IN RADWASTE MANAGEMENT A NON-PROFIT ORGANIZATION

[DATE]

Subject: Notification of potential breach of credit card information related to WM2022 registration platform during the period 1 January 2022 through 20 April 2022.

Dear WM2022 Conference Registrant:

We are writing to advise you of an incident that may have affected your credit card number.

What happened?

We have been advised that X-CD, a service provider that operates the WM Symposia, Inc. (WM Symposia) conference platform system, discovered malicious code in its software that may have compromised the credit card data of individuals that accessed the platform from the period 1 January 2022 through 20 April 2022. X-CD handles all credit card payments for us; WM Symposia does not receive, collect, store, or process your credit card information. WM Symposia is committed to the security of our conference platform users, and we have taken steps to prevent future breaches of the conference platform system.

What information was involved?

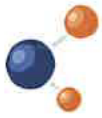
As soon as we learned about this incident and that credit card data may have been affected, we began a thorough investigation and have pressed X-CD to do the same. We recently received a copy of X-CD's report. Our records indicate that you accessed the conference platform system during that time. X-CD has not been able to identify whether your credit card was compromised, and we are providing this notice out of an abundance of caution.

What we are doing.

WM Symposia has:

- Required and confirmed that X-CD discontinue use of its previous payment processing module and instituted use of Authorize.net for processing of credit card payments; this prevents X-CD access to any credit card information
- Required X-CD to conduct a full forensic review to identify the cause and scope of the incident
- Received assurance from X-CD that they have successfully removed the malicious code from their software
- Hired a cybersecurity subject matter expert to (a) evaluate and update WM Symposia security procedures and (b) evaluate the X-CD conference platform
- Updated all passwords and VPN access for all WM Symposia personnel
- Conducted a vulnerability assessment for our WM Symposia personnel computers and systems
- Hired a Chief Information Security Officer (CISO) to evaluate the WM Symposia systems for security issues on a regular basis

What you can do.



- Remain vigilant for incidents of fraud by reviewing your account statements and monitoring your free credit reports
- Report any suspicious activity or transactions to your bank.
- Learn about steps you can take to protect yourself from identity theft by visiting the Federal Trade Commission's (FTC) Web site, at www.consumer.gov/idtheft, calling the FTC, at (877) IDTHEFT (438-4338) or writing to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
- Periodically obtain free credit reports from each nationwide credit reporting agency by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies so you may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period.
- Contact the credit reporting agencies to report fraudulent transactions or incorrect information at:

Equifax
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com.

For more information.

You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file that tells creditors to follow certain procedures to help protect your credit information. Just call one of the three nationwide credit reporting agencies listed above, it will notify the other two agencies. A fraud alert may delay your ability to obtain credit. You can also contact the credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit them from releasing information from your credit report without your prior written authorization.

Please know that WM Symposia sincerely regrets any inconvenience or concern this incident has caused. If you have any questions related to this incident, please contact us directly at +1.877.849.6400 or by email at info@wmarizona.org.

Sincerely,

Susan A. Walter
Managing Director, WMS

Susan Stiger
President, WMS

CALIFORNIA RESIDENTS: California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Please see above for obtaining your free credit reports. For

more information on identity theft, you may visit the California Office of Privacy Protection website, www.oag.ca.gov/privacy.

INDIANA RESIDENTS: please read the Indiana Identity Theft Prevention section online at www.IndianaConsumer.com for more information about steps you can take and situation-specific actions and responses.

IOWA RESIDENTS: To report suspected incidents of identity theft contact local law enforcement or the Iowa Attorney General's Office at Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, http://www.iowaattorneygeneral.gov/.

MARYLAND RESIDENTS: Obtain information about avoiding identity theft from the FTC at the address above or the Maryland Attorney General's Office at Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

NEW YOR RESIDENTS: Visit the New York State Consumer Protection Board website at www.dos.ny.gov/consumerprotection for more information on identity theft.

NORTH CAROLINA RESIDENTS: obtain information about preventing identity theft from the FTC at the address above or the North Carolina Attorney General's Office at North Carolina Department of Justice, Attorney General Josh Stein, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226, http://www.ncdoj.com.

WEST VIRGINIA RESIDENTS: You have the right to obtain a security freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer-reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer-reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer-reporting agency; (2) Proper identification to verify your identity; and (3) The period of time for which the report shall be available to users of the credit report.

A consumer-reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. A security freeze does not apply to circumstances in which you have an existing account relationship, and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit. You have the right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer-reporting agency.