EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MW Industries does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2020, MW Industries discovered a file containing personal information related to certain MW Industries' employees was made available via a public website, justanswers.com. MW Industries immediately launched an investigation, with the assistance of a leading forensic investigation firm, to determine when and how this file was posted on the website. This investigation is on-going, and, to date, the exact date of the posting is not confirmed. In coordination with the forensic investigator, MW Industries worked to have the information removed from the website, which occurred on October 7, 2020. Based on the investigation to date, it is believed the file was posted to this website by a former employee and was not the result of a system intrusion or other unauthorized access to the MW Industries network.

The personal information that could have been subject to unauthorized access includes name, Social Security number and financial account number.

Notice to Maine Resident

On or about November 3, 2020, MW Industries began providing written notice of this incident to all affected individuals, which includes one (1) Maine 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, MW Industries moved quickly to investigate and respond to the incident, assess the security of MW Industries systems, and notify potentially affected individuals. MW Industries is also working to implement additional safeguards and training to its employees to help ensure that a similar situation does not occur in the future. MW Industries is providing complimentary access to credit monitoring and identity theft recovery services for 12 months, through ID Experts, to MW Industries employees whose personal information was potentially affected by this incident.

Additionally, MW Industries is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with 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.

EXHIBIT A

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit: https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 3, 2020

RE: <<Variable subject line>>

Dear <<First Name>> <<Last Name>>:

The ASP MWI Holdings Inc. d/b/a MWI Industries ("MW Industries") writes to inform you of an incident that may affect the privacy of some of your personal information. We take this incident seriously and are providing you with background on the situation and steps you can take to better protect your information, should you feel it is appropriate to do so.

What Happened? On October 2, 2020, we discovered a file containing personal information related to certain MW Industries' employees was made available via a public website, justanswers.com. We immediately launched an investigation, with the assistance of a leading forensic investigation firm, to attempt to determine when and how this file came to be posted on the website. This investigation is on-going and, to date, the exact date of the posting is not confirmed. In coordination with the forensic investigator, we worked to have the information removed from the website.

What Information Was Involved? Our investigation determined that the file may have contained your name, Social Security number, HSA account number, employee identification number, and financial account number.

What We Are Doing. In addition to our ongoing investigation, we are providing notice of this incident to you, as well as access to information and resources to help protect your information, should you feel it appropriate to do so. While we are unaware of any evidence of actual or attempted misuse of your information at this time, as an added precaution, we are also providing you access to <<service length>> months of complimentary credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services through IDX. Upon completion of the investigation, we will take any and all actions necessary to help ensure that a similar situation does not occur in the future.

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 activity and to detect errors. You can also enroll to receive the complimentary monitoring and restoration services we are offering at no cost to you. Instructions on how to do so, and other helpful information, can be found in the enclosed "Steps You Can Take to Protect Your Information." Please review this information for additional steps you can take to protect your information from misuse.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at (800) 939-4170 from 6 a.m. and 6 p.m. PST, Monday through Friday.

We take the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Shelley Garrity
Chief Human Resources Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Monitor Accounts

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
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
1-800-685-1111
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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	www.equifax.com/personal/credit-report-services

Additional 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); and 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [XX] Rhode Island residents impacted by this incident.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

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 violator. 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.

Oregon residents, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/; 877-877-9392.

Kentucky residents, Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov; 1-502-696-5300.

For District of Columbia residents, the Office of the District of Columbia Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov; or you may visit the website of the Office of the District of Columbia Attorney General at https://oag.dc.gov/.