Associated Management Services
Associated Employers
2727 Central Ave, Suite 2
Billings, MT 59106
www.associatedemployers.org

June 24, 2019

We are contacting you about a data breach that has occurred at Associated Management Services and Associated Employers.

On Friday, June 14, 2019, we discovered that many of the Associated Employers' servers in our office, including replica servers and backup servers along with our online offsite back-up service had been compromised by Ransomware.

The management Board of Directors (AMS) and the related entities' board chairmen were immediately notified. Our local IT consulting firm and AE management team worked tirelessly through the weekend and following week to use all means possible to recover, unencrypt and to restore services. On the Monday morning after the attack, we were able to fully recover and use our entire payroll operating databases without data corruption. We also were able to use most of our other operating databases with only one day of data loss.

In terms of our operating websites, this breach did not affect www.SlatePayroll.com, www.GraniteHR.com, www.JobJupiter.com, www.AssociatedEmployers.org, www.MSSC.org or www.AETrust.org as they are not on our local servers and do not use the online backup service that was hit with the Ransomware.

This breach did delete, corrupt or encrypt our internal production server and files, along with our www.amstime.org and www.lab.mssc.org websites. We will no longer offer www.amstime.org as a service as our modernized and secure option is www.slatepayroll.com.

We are seeking expert advice along with our internal IT employee and our local IT consulting firm to try to determine what occurred and how Ransomware attacked some of our servers, replicas and backup servers. We are also researching expertise outside of Billings Montana to assist us with security.

We did contact the FBI Cyber Crimes unit and reported the incident for their use.

At this point, we cannot say with certainty whether the Ransomware hackers took any data to utilize versus just deleting and encrypting data a with a Ransom attack. We have not received any indication that the information, if obtained, has been used by an unauthorized individual but we must take all precautions. Information that could have been obtained may have included personal information such as name, address, social security number, date of birth and bank account numbers.

We recommend that you and your employees change your bank account numbers, passwords and place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax:	equifax.com	1-888-548-7878

Experian:	experian.com	1-888-397-3742
TransUnion:	transunion.com	1-888-909-8872

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the number above to place a free credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name.

For additional information please go to associatedemployers.org/news. On our website, please find a copy of *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

We are very sorry that Ransomware hackers were able to hit our system and apologize for any inconveniences this may have caused.

Sincerely,

Greg Roadifer

Greg Roadifer
President