MUNICIPAL FIRE AND POLICE RETIREMENT SYSTEM
CLOUD SERVER BREACH TIMELINE
February 6, 2017

Municipal Fire and Police Retirement System (the "System") maintains a secure website for city fire and police department employers to submit beneficiary wage reports and to submit ACH payments. Byrne Software, Byrne Software provides the software for the web hosting facility. The web hosting facility is currently located on a Rackspace virtual server. The cloud server is not on the System's site in West Des Moines but is instead accessed through an internet connection. Client governmental entities access the cloud server through a Byrne Software web portal that runs on the cloud server.

On Thursday, January 26, 2017, Byrne Software notified Dan Cassady, Deputy Director at the System that the cloud server had been encrypted by a ransomware program. The ransomware had a run date of January 21, 2017. Information on this cloud server included beneficiary social security numbers and names. No personal account numbers are believed to be on the wage reports. Assuming that every possible participant was in the reports, out of a total of 25 states, there are 4,112 beneficiaries from Iowa, 26 from Nebraska, 20 from Illinois, 13 from Minnesota, 7 from Wisconsin, 6 from South Dakota and 5 from Colorado, with the remaining beneficiaries scattered in 18 other states in numbers between 1 and 4 each. On Thursday, February 2, 2017, the System's insurance company approved a statement of work prepared by Integrity Technology Systems, Inc. and Integrity began investigating the server.

On Saturday, February 4, 2017, Integrity discovered that Remote Desktop Connection (Terminal Services) was enabled for all incoming internet connections. Also, the password policy and account lockout policies were not enabled which makes the system susceptible to brute force attacks. During the subsequent log review, Integrity discovered successful remote desktop connections using the administrator account from the countries of Bulgaria on 1/20/2017, Iran on 1/18/2017, Great Britain on 1/6/2017 and various sessions from US-based locations using Windstream Communications, Verizon Wireless, and CP Internet IP addresses. Other sessions are evident, including an unsuccessful brute force attack from China.

According to Integrity, the current evidence suggests the last attack from Bulgaria was the source of the ransomware. It is unknown at this time if this was the sole intent of the attack or if it was used to hide evidence of other malicious activity. No anomalies have been noted on the System main servers.

The System is assuming the names and social security numbers have been compromised. Counsel for the System will follow each state notification requirements and provide notice to affected beneficiaries once the System gets approval from law enforcement. The System will continue to work with its security consultant to examine a bit-level copy of the cloud server to obtain more information on the nature of the attack and if there is any evidence of what the attackers may have copied or done while they had VPN access. The consultant will also review the network configuration at the main System office to determine if that separate system has any vulnerabilities.