Dave Yost • Auditor of State

TO: **UAN Clients**

FROM: **UAN Support**

DATE: **June 20, 2016**

SUBJECT: **UAN Guidance for Clients Encountering Malware**

Much like many other computer users, the clients of UAN have seen an increase in malicious software attacks to their UAN computers including ransomware. The purpose of this document is to inform UAN clients of the actions that UAN Tech Support may take when a UAN client has been affected by one of these attacks.

- UAN Tech Support will continue to give the entity its options on how to resolve any problems that arise from software attacks on the UAN computers. However, UAN staff cannot give advice on whether an entity "should" pay a ransom or fee to a criminal hacker. Whether to pay a ransom or fee is a decision that rests solely with the public office after consideration of all the issues and seeking advice of counsel. While it may be the only option the entity has for retrieving data, it must be the entity's decision whether to proceed or not with paying a ransom.

UAN has been informed by AOS Legal and Audit that we may communicate that if the entity has applied general safeguards to secure public records, generally, the AOS will not issue FFRs against entities or fiscal officers who find themselves to be the victim of criminal hacking, malware, ransomware and various other computer viruses caused by criminal activity and if the public office has funds stolen as a result of the attack or finds it necessary to pay a ransom in order to retrieve data and other necessary digital information.