Oregon, Tillamook, January 23, 2020 – Tillamook County is experiencing difficulties with our computer resources including interruptions in systems and services. These difficulties are caused by malware – bad computer code – that encrypts data files on our computers.

With the help of a digital forensics incident response team, and law enforcement, we are investigating the incident and working toward recovering operations. Although the investigation by our digital forensics team is underway, we have no evidence at this time that there has been a breach involving the unauthorized access or taking of sensitive data. Should the forensic investigation determine there was a breach, the County will then determine what information was accessed and provide any necessary consumer or regulatory notifications at that time.

Timeline of the Incident

On January 22, 2020, Tillamook began to experience computer difficulties which affected several of its computer systems. Tillamook determined that the malware had begun to encrypt its network and immediately began to disconnect its workstations and servers to halt the encryption attack. The encryption means that the data files cannot be accessed by anyone until they are unencrypted – or unlocked – with a decryption key. According to information provided by law enforcement, it would take approximately twelve (12) years for current generation supercomputers to decrypt the data without the decryption key.

It is important to understand that the data was not removed from the County's systems. The malware operated within the County's computer environment encrypting the data files on the County computers. Law enforcement and our digital forensics team inform us that this is consistent with the behavior of the actors who use this malware.

The County's next step was to report the incident to our cyber insurance carrier. We then engaged the Data Privacy and Cyber Security team at Lewis Brisbois Bisgaard and Smith ("Lewis Brisbois") to oversee the forensic investigation and to coordinate with law enforcement. We also retained a leading forensics firm Arete Advisors ("Arete") to obtain the decryption key - if necessary, to perform the forensic investigation, determine the root cause of the incident and provide assistance with mitigating the risk of future incidents. The County is determining whether viable backups can be used to restore the encrypted data.

The County will have more information when the investigation is completed. We are exploring security enhancements with our digital forensics team. In the meantime, we appreciate everyone's patience as we restore our computer operations.

Thank you.