PHASE TWO REPORTING INFORMATION

A. Incident Response Associated Information (Additional Details)

1. To the extent you are able at this point, please provide more specific details relating to the *incident timeline* from the time of initial intrusion, identification and key points relating to the extent of compromise known to date.

2. To the extent you are able to at this point, please provide any details related to the characteristics of the intrusion known to date. (Examples – indicators of compromise; tactics, techniques and procedures employed to gain access and infiltration). If it is too early to provide those details, they can be provided at a later date.

3. To the extent you are able to, please provide copies of any relevant log files on the network relating to this incident. If it too early to provide those details, they can be provided at a later date.

4. To the extent you feel comfortable with sharing, please provide any incident response reports available relating to the incident – either internally generated or those provided by 3rd party contracted support. These could also be provided at a later date.

B. Threat Vector Details (Additional Details)

1. Are there any details relating to the specific method used to gain access and any associated characteristics of the system intrusion?

2. Are there any additional details that can be provided relating to the threat actor(s) based on interactions to date?

3. Have the threat actors provided any account details or transaction instructions?

4. Are there any specific attributions recognizable as associated to the threat actors?

5. Are there any key virtual currency addresses and activities of note related to this incident?

6. Do you have any further information that may lead to an understanding of who may have taken this action against your organization?

C. Ransomware Incident Specific Information

1. Are there any additional data artifacts of note related to the incident?

2. Has a ransom been paid?

i. If so, can you provide any details associated with the payment process that was followed during the incident?

ii. If considering payment, can you provide any process-related information associated with the upcoming transaction?

D. Other incident related information not yet provided

1. Is there any other information, process-related or technical, not yet covered which you feel is important for police to be aware of at this time in order to gain a deeper understanding of the incident?

2. Are there any other external 3rd parties engaged at this point that have not been identified with whom you believe police would benefit from speaking to?

3. Are there any external support requirements for victim services that your organization and/or personnel within may benefit from being connected with to assist with managing the consequences and impact of the incident?