FAQs for the MICROS Security Incident

1. What is the plain English explanation of the incident?

Oracle Security has detected and addressed malicious code in certain legacy MICROS systems. Upon the discovery of this code, Oracle security teams worked to identify impacted systems and block malicious processes and unauthorized network connections. To prevent a recurrence, Oracle implemented additional security measures for the legacy MICROS environment.

Consistent with standard security remediation protocols, Oracle is requiring MICROS customers to change the passwords for all MICROS accounts.

2. Were Oracle systems impacted?

Oracle's Corporate network and Oracle's other cloud and service offerings were not impacted.

3. Is Payment Card data encrypted in MICROS hosted customer environments?

Payment card data is encrypted both at rest and in transit in the MICROS hosted customer environments.

4. What actions is Oracle requiring in response?

Oracle is requiring MICROS customers to change their passwords for all MICROS accounts. Information for customers on how to change their passwords has been published on My Oracle Support (Doc ID 2165744.1). Oracle will force a password change in hosted MICROS systems where possible. We also recommend that you change the password for any account that was used by a MICROS representative to access your on-premises systems.

5. Was my data impacted?

In the event that Oracle determines that your data was impacted, Oracle will contact you directly.

6. Who can I contact if I have additional question(s) about this incident?

Please refer to My Oracle Support (Doc ID 2165744.1) for additional information. If you have additional questions or concerns, you may contact MICROS Support at http://www.oracle.com/us/corporate/acquisitions/micros/support/index.htm.