POS Incident Response – Operator

Introduction

The following process should be followed in any situation where a consumer or operator feels there has been a security incident with a market. This process is meant to help gather data that will be passed to the 365 Retail Markets Incident Response Team (IRT) for review. In all situations it is important to contact 365 Support to have the situation documented and a case created for investigation. ***This is essential to demonstrate that 365 Retail Markets and you (the operator) have exercised due diligence to protect the consumer PII and Card Holder Data.***

Process

1. Contact 365 Support at **888-365-6282** and open a ticket with the initial information supplied by the host location.

2. Contact the person(s) reporting the incident and complete the "Consumer Incident Questionnaire" and send it to Support or Security.

3. Provide a full list of potential consumers who may have been impacted by the reported incident. If several people refuse to provide the information for the "Consumer Incident Questionnaire" at least provide the User name(s) and the total number of impacted consumers.

4. Using the appropriate "Physical Security Audit", review the device at the host location for any tampering. Take photos of the components listed below and provide them to the 365 Security Team.
    - Outside of Credit Card Reader
    - Kiosk Lock / Encasement (where applicable)
    - Inside of Credit Card Reader (where applicable)
    - Card Reader USB cable (where applicable)
    - Screen of device if the 365 Application is not displayed

5. Review the DVR footage. When an incident is reported, it is vital that the video footage be reviewed to verify the date and time the incident was reported or suspected to have occurred. If no DVR is in place, you (the operator of the kiosk) should contact the local company and request that this footage be reviewed, and the same process followed.

Based on device accessibility, 365 Security may request that the device be replaced. This is not an indication of an actual incident, but it may speed up the incident response process.

In some situations, you may decide it is necessary to replace the device to build confidence with the host location. To do so, contact 365 Support to schedule the process. This is only recommended in specific situations, and you should exercise caution. Some consumers may view a computer replacement as an indicator of an incident, even if one did not occur.

If an actual incident did occur, the 365 Retail Markets IR team will contact the you to discuss the appropriate disclosure process that follows local and state laws.