

Data Security Breach Action Plan

It can be difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion can be challenging. If during your normal operations you suspect there is a problem with your security, a customer advises you that their credit card information has been compromised, you are contacted by law enforcement, your financial institution, or processor of a possible breach, then immediate action should be taken. Therefore, if at any time a security breach is suspected the following steps should be taken.

- Do not alter the compromised system in any way.
- Do not change and passwords.
- Do not turn the system off.
- Discuss and review your findings with your immediate supervisor.
- Preserve all logs.
- Document all actions including the exact date and time of the discovery.
- Contact your POS Support organization for assistance.
- Take immediate action to contain and limit the exposure by isolating the compromised system, i.e. unplug the network cable disconnecting the system from the Internet.
- Do not take any other action. Contact the Merchant Bank, processor, Card Company, and appropriate law enforcement agency.
- Review Card Company requirements for reporting and compliance.