Responding to a Breach:  
A Guide Provided by Bank of America Merchant Services

Suspect that your business has experienced a data security breach? Please take advantage of these step-by-step instructions for tips on how to manage the incident:

1. Immediately contain and limit the exposure. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. To preserve evidence and facilitate the investigation:
   - Do not access or alter compromised systems (i.e., don’t log on to the machine and change passwords, do not log in as ROOT).
   - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
   - Preserve logs and electronic evidence.
   - Log all actions taken.
   - If using a wireless network, change the Service Set IDentifier (SSID) on any access point or any other devices that may be using this connection with the exception of any systems believed to be compromised.
   - Be on “high alert” and monitor all systems with cardholder data.

2. Alert all necessary parties immediately. The card organization rules and regulations require that all data security breaches involving card holder information be reported.

   Be sure to contact:
   - Merchant Services from Bank of America (through your account manager, if applicable, or Customer Service at 1.800.228.5882)
   - Local law enforcement and the local office of the United States Secret Service

3. Be prepared to provide all compromised card accounts to Bank of America upon request.

4. Provide an Incident Response Report within three business days of the reported compromise.

5. Contain/control the event per Visa’s Cardholder Information Security Protection (CISP) and MasterCard’s Site Data Protection (SDP) program guidelines.

6. Be prepared to hire a certified third party vendor to conduct forensic investigation if required. Upon request, forward forensic investigation report to Bank of America.

7. Schedule validation of Payment Card Industry Data Security Standard (PCI DSS) examination and system scan. The scan must be conducted quarterly. Upon request, be prepared to forward results to Bank of America.

To obtain information on the PCI DSS go to: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). You can also read more about validating compliance with the PCI DSS on [www.bankofamerica.com/pci](http://www.bankofamerica.com/pci).