In the event of a POS system data breach,

**perform the following steps immediately.**

# Determine the extent of the breach.

* + Which systems or networks were compromised?
  + What information was accessed?

# Notify the affected customers and employees.

* + Inform them how, when, and in which location(s) their information was stolen.
  + Recommend that they secure their accounts and information via changing passwords and double- checking their purchase histories.

# Consider offering identity theft protection to your customers.

* + A year or more of protection would help repair your reputation.

# Hire a cybersecurity firm.

* + Have the firm investigate the breach and recommend further security measures. You may want to keep customers informed of this investigation’s progress and results.

# Keep track of all communication and activity related to the data breach.

* + This will be useful both for the cybersecurity firm’s data-gathering as well as for legal evidence if necessary.
  + Track and preserve all records of communication and activity relevant to the data breach, such as: Email, phone, or online chat correspondence

Any recorded connection or access to your infrastructure, whether by internal or external users POS systems transaction records

Bank statements and credit card batch processing records

# Contact the Federal Trade Commission (FTC) law enforcement, and credit bureaus.

* + Credit bureaus can help businesses protect their customers’ credit information.

# Contact your insurance company.

* + They may be able to help you recover some of your financial losses.

