What can you do?

Business Owners:

1) Ensure that your Business is PCI Compliant (www.pcisecuritystandards.org). Review the PCI Self-Assessment Questionnaire (https://www.pcisecuritystandards.org/saq/index.shtml) which shows if your business is currently meeting PCI standards. Some of the important PCI Principles to consider include:
   A. Build and Maintain a Secure Network
      a. Install and maintain a firewall configuration to protect cardholder data
      b. Do not use default or simplistic system passwords
   B. Protect Cardholder Data
      a. Encrypt transmission of cardholder data across open, public networks
   C. Maintain a Vulnerability Management Program
      a. Use up-to-date anti-virus software and set it up for automatic updates
   D. Regularly Monitor and Test Networks
      a. Track and monitor all access to network resources and cardholder data
      b. Regularly test security systems and processes
   E. Maintain a policy that addresses Information Security
2) Ensure that the person(s) who handle your Information Technology (IT) have completed the work that was requested. (Many times a business will purchase the most up-to-date software versions, but will not receive them in a timely manner.)
3) Make sure that your Point of Sale software is currently running the most up-to-date version. (Usually a new version of software becomes available when there are known vulnerabilities that need to be patched.)
4) Carefully review your business network incoming traffic but, equally important is reviewing your outgoing traffic to ensure no customer data is being infiltrated.

Consumers:

1) Check your banking and credit card transactions frequently. (The sooner you identify fraud on your account, the sooner the illegal activity can be stopped.)
2) Obtain a police report for your records.
3) Contact your financial institution and determine what alerts and/or services are available to notify you of suspicious transactions as they occur. An ounce of prevention is truly worth a pound of cure here….

Financial Institutions:

1) Ensure the policies and procedures are in place to rapidly contact your credit card processor to stop fraudulent charges once a victim business is identified.
2) Maintain close contact with Security Officers and Risk Management employees at local Financial Institutions. Join the Financial Institution Security Officers Association (FISOA) or a similar organization and become an active participant at the meetings (www.safecityabq.org).
3) Look for trends in reports of fraud such as a "common point of purchase" and notify your local law enforcement when a new trend is discovered (i.e. www.cabq.gov/police, www.secretservice.gov, www.ci.rio-rancho.nm.us, www.FBI.gov, and www.bernco.gov/live/departments.asp?dept=2318).