Policy for Protecting Customer Data

Store Name _____

Store Owner/Manager _____

Date Accepted _____

Protecting our customer and employee information is very important to our store image and on-going business. We believe all of our employees must actively participate in keeping our customer information private and secure.

Customer and employee data - customer or employee name in association with cardholder data, driver's license number, check or bank account numbers, PIN numbers, or any other information that could be used fraudulently to harm customers.
Cardholder data - customer name in association with the full credit card number, PIN number, and other credit card information used for authorization.

1. The store is responsible for having policies and procedures in place for the physical, operational, and electronic protection of customer and employee data. The policies and procedures will be reviewed when there are changes to the customer data being used or stored, and at least annually.
2. All policies must be incorporated into daily procedures and practices, as well as reviewed with employees at time of hire and at least annually. All relevant policies must be shared with vendors and other third parties that have access to customer and employee data.
3. The store manager is responsible for data security at the store, including providing on-going data security awareness training to employees and monitoring and sharing relevant trade information about data security,
4. All employees must use reasonable care and common sense to protect customer and employee data. Employees are required to agree, in writing, their understanding of these requirements and agree to follow store policies.
5. Access to customer and employee data, with an emphasis on cardholder data, must be restricted to those employees with a business need-to-know. Those employees allowed to access systems with customer and employee data must have a unique ID and password.
6. Employees are not allowed to add personal devices or software to store systems. All new software, hardware and/or other component changes to systems with customer and employee data must have management approval.

All third-party vendors must review software and hardware changes with management when making changes to applicable systems.

7. Customer data, particularly cardholder data must be encrypted when it is sent over the public internet, including in emails. When displayed all credit and debit card numbers must be masked to display the last four digits. Storage of customer and employee data should be kept to only what is necessary for business, legal, and/or regulatory purposes.
8. Cardholder magnetic stripe data, including full track data, card-validation code, and PIN must never be kept in store systems.
9. All systems with customer and employee data must be properly installed and maintained according to store written practices, vendor supplied guidelines, or other provided guidelines. Guidelines will include a requirement to change all vendor supplied default passwords. These systems must have adequate protection to minimize the risk of theft, tampering and/or accidental exposure of data.
10. All systems that contain customer information, particularly cardholder data, must be reviewed annually to insure procedures are in place to minimize the risk of fraud, theft and unintended exposure of data. Store managers must be aware of current threats and vulnerabilities to these systems.
11. Systems with customer and employee data that are susceptible to malicious software and other vulnerabilities must have up-to-date anti-virus software, application and operating systems updates, and security patches.
12. If public internet connections, the store must have adequate network protection in place to protect against external attacks, including the use of firewalls, intrusion protection and other security controls.
13. The store will test applicable IP based systems for security controls on a quarterly basis, including internet facing systems, internal systems, and wireless network devices.
14. All paper and systems that contain customer and employee data must be physically secured. Backup media that contains cardholder data must be stored in a secure location. All systems that contain customer and employee data must have management approval before moving components from their secure location. Customer and employee data on paper documents and electronic systems must be made “unreadable” before disposal.
15. All service providers/technicians must have prior management consent before accessing any systems with customer and employee data. All employees are required to verify service providers/technicians identity prior to accessing systems.
16. The store will have an incident response plan in place with contact information and escalation requirements in the event any customer or employee information is lost, stolen or accidentally exposed.

SECURITY AWARENESS TRAINING

Keep your data safe… keep your customers' data safe.

What can you do to protect your store and your customers from credit card thieves?

1. **Protect your customer's personal information.** This may seem simple, but protecting your store from the risks and pitfalls that come from credit card fraud and customer identity theft is really about keeping your customer's information private. If your store is involved in the loss of credit card numbers, the store could see huge fines. If customer personal information is involved, there could be costly state requirements and legal costs. Protect your store by protecting your customer's personal information.

2. **Don't share your access to store systems.** Sharing your sign-on and password may seem like "no big deal" but the store's point-of-sale system is set up to only give you the access you need – no more, no less. Sharing your sign-on would be like giving someone else access to your ATM card. Sure, they're your friend, but you don't know if they are going to pull out $20 or your car payment.

3. **Confirm credit card numbers are not printing on customer or store receipts.** Here's an easy one that makes a big difference to your store. Make sure full credit card numbers are not printing on receipts. Not only is this a federal requirement, but it means that credit card receipts can be thrown in the trash. Receipts should only show the last four digits of a credit card and should not include the expiration date.

4. **Verify the identity of any technician that wants access to store systems.** Stealing customer information has become a business. And in known cases, thieves are pretending to be service technicians asking to upgrade or replace POS systems, debit card entry pads, and even asking to access the gas pumps. If anyone wants access to your store's systems, call your store manager and ask the technician for identification and verification.

5. **Don't put paper or computers with customer information in the trash.** Customer and employee information that could be used for fraud or identity theft must never just be thrown in the trash. Documents with customer name, full credit card numbers or any other personal information must be shredded or destroyed so the information can not be illegally used. Computers with credit card information must not be thrown in the trash either. Talk with your store manager about how to get rid of journal tapes, employee information, and computer systems.

6. **Look for tampering on pumps, ATMs and other systems that accept credit cards.** One of the ways thieves are stealing customer credit card information is by planting extra devices on pumps, ATMs, and other systems that handle PIN numbers and credit card transactions. These devices can be installed inside of a pump, on the front of a pin pad, or even on a wire in the point-of-sale terminal. Know what your store systems should look like and look for tampering daily. If you suspect there is a problem, call your store manager.

7. **Don't plug personal and unsafe devices into the store systems.** Never add your personal devices – iPod, laptop computer, wireless access or any other devices – to your store's computer systems or network. Unsecured, unknown devices added to the store network may cause everything to stop working and it could make it very easy for thieves to steal credit card data.

8. **Don't add software to store computers.** Adding software to computers can cause huge problems. Some software, malicious software that steals customer and employee information, is especially crafted to be easy to install and may seem harmless. Stores have lost thousands of credit card numbers after having software installed on point-of-sale machines. Even something as simple as an internet toolbar can have bugs that make it easier to steal information.

9. **Know who to contact if there are problems at the store.** If you suspect there is a problem with credit card fraud, equipment tampering, or suspicious vendors contact your store manager. Your store should have an Incident Response Plan. Know where it is, review it with your store manager, and use it if you have a problem.

I understand that I play a huge part in protecting our store's systems and customer information. I have read the steps I need to take every day to keep customer information secure.

_____ Employee Name _____ Date _____ Store Manager Initials

Procedures for protecting customer data

Store Name _____

Store Owner/Manager _____

Date Accepted _____

To help you and your employees protect customer data, these easy to follow procedures should be incorporated into your daily business practices.

- Train employees to combat credit card fraud by verifying the following for in store transactions:
  ___ Customer name on credit card matches customer name on receipt.
  ___ Signature on the card signature panel matches the signature on the receipt.
- Verify credit card numbers are masked on all customer receipts (by law the last 4 digits may show without the expiration date.). If applicable, verify credit card numbers are being masked on all store reports. Including:
  ___ Journal tapes
  ___ Backup credit card batch file
  ___ Other _____
- Keep a "store log" to document daily practices are occurring, track visits by technicians and other critical third-parties, note updates to point-of-sale and other important systems, and record any security situations that may impact customer data.
- Keep copies of service tickets/receipts to record changes, updates, installations and all services performed on point-of-sale, communication, and other devices that may have customer data. Records should include impact to current environment, resolution if there is a problem and initials of store manager.
- Verify paper documents are securely stored and properly disposed of:
  ___ Receipts/documents with credit card numbers are locked in the manager's office with limited access by employees.
  ___ Receipts/documents with customer information are not thrown in the trash when no longer needed.
- Verify all systems that accept credit cards are adequately secured against physical removal.
  ___ No unknown devices connected
  ___ No devices attached to USB ports (check both front and back of POS)
- Verify that all pump access doors to the credit card readers are locked and have not been tampered with (tamper proof tape on access doors daily will assist with this).
- Physically inspect all CRIND (Card Reader In Dispenser) devices daily to look for unknown (skimming) devices that may have been added.
- Verify that all security cameras are pointed at the appropriate locations and can not pick up customer information, including credit card data or PIN (Personal ID Number).
- When disposing of point of sale equipment, the hard drive needs to be taken out and destroyed.

Third-party access to store systems

Store Name _____

Store Owner/Manager _____

Date Accepted _____

Third-parties managing and maintaining our store systems have a duty to protect customer and employee information when it is in their care. The store will maintain a list of all service providers and their agreement to protect customer and employee data, including their PCI compliance status.

Customer and employee data - customer or employee name in association with cardholder data, driver's license number, check or bank account numbers, PIN numbers, or any other information that could be used fraudulently to harm customers.
Cardholder data - customer name in association with the full credit card number, PIN number, and other credit card information used for authorization.

1. Third-parties, including vendors, contractors and service providers, have the same responsibility to adhere to the security standards for protecting customer and employee information that the store follows. This includes, but is not limited to PCI-DSS requirements (Payment Card Industry Data Security Standards) for handling credit card data.
2. Access to customer and employee data and the systems that process, transmit and/or store that data will be limited to those third-parties that have written agreements to manage and/or maintain those systems.
3. Third-parties that manage and/or maintain store systems must consider and preserve the security and integrity of all store systems with customer and employee information when adding, changing, or removing hardware and software required for their system.
4. Third parties agree to take reasonable steps to protect customer and employee data, including credit card data, while the data is in their possession. This includes any data on systems being transported, managed, and maintained by the third party. When the data is no longer necessary for business purposes, the third party agrees to securely dispose of the data.

Third Party Name _____

Third Party Company _____

Date Accepted _____

Data Loss Response Plan

The Data Loss Response Plan outlines the steps to be taken in the event of loss or theft of customer data, including credit card data.

Store Name and Location _____

Store Phone Number _____

Store Manager/Primary Contact _____ Cell Phone _____

Alternative Phone _____ (home/other)
(This person is the primary contact who will act as the spokesperson for the store. He/she should be available 24/7 to respond to any data loss and to help determine escalation procedures.)

Loss of Customer and/or Employee Data:

1. Contact local authorities first if theft, bodily harm, or vandalism is involved.
   - If IP based systems are involved, contain and limit the exposure of customer and employee data by removing any compromised systems from having public internet access.

2. Contact your store manager/primary contact to discuss what data was lost, stolen and/or accidentally disclosed.

3. The store manager will be responsible for contacting store management (store owners/company management) to determine next steps.

4. If cardholder data is involved, store management must contact Sinclair Marketing Offices and be prepared to contact the processing bank for instructions on next steps. Visa Investigations and Incident Management Group will need to be involved, as well as Fraud Investigation Groups for other credit card companies.

5. Store management should familiarize themselves with state laws for customers regarding reporting the loss of customer information.

6. Store management should have a plan for communication to customers, media, and local officials if necessary.

Sinclair Marketing Office, System Support	(800) 524-4799
First Data / Buypass Help Desk	(800) 726-2629
Visa Investigation and Incident Management	(650) 432-2978

Detailed Report

The store manager should be prepared to provide a detailed report of what happened, who was involved, what data was compromised, and what steps employees took to reduce the exposure. The store must keep a copy of the report with other PCI Program documentation.

Lessons Learned

The store manager should review the actions taken after a data compromise with all employees, update the response plan, polices and other procedures as needed.

Annual Review

The store must review the Data Loss Response Plan on an annual basis, and confirm that all employees are know what is involved in a data compromise and who they should contact.

Data Plan Reviewed with Employees _____