NH DEPARTMENT OF CORRECTIONS POLICY AND PROCEDURE DIRECTIVE	CHAPTER Financial Services STATEMENT NUMBER 3.19
SUBJECT: ***GraniteCor* - RETAIL SHOWROOM -PAYMENT CARD INDUSTRY COMPLIANCE** PROPONENT: William McGonagle, Assist. Comm. *Name/Title* Commissioner's Office 271-5601 *Office* *Phone #*	EFFECTIVE DATE 01/15/13 REVIEW DATE 01/15/14 SUPERSEDES PPD# 3.19 DATED 03/01/08
ISSUING OFFICER: *William Wrenn, Commissioner*	DIRECTOR'S INITIALS: DATE: APPENDIX ATTACHED: YES NO
REFERENCE NO: See reference section on last page of PPD.	

I. PURPOSE:

To establish guidelines for the operation and management of GraniteCor's Retail Showroom, and to ensure that electronic payments are in compliance with Payment Card Industry (PCI) standards, and to assign authority and responsibility for processing electronic payments at the Retail Showroom and for accepting checks for Hay, Wood, Plants, and Picnic Tables at the Farm.

II. APPLICABILITY:

This policy applies to GraniteCor staff involved in the operation of the Retail Showroom including those responsible for records, deposits, reports, bank coordination, and staff having a business relationship with the Store.

This policy applies to payments made to GraniteCor with check or credit card. The Retail Showroom has one electronic processing machine used for GraniteCor transactions (see IV B 3).

III. POLICY:

It is the policy of the NH Department of Corrections that:

A. The GraniteCor Retail Showroom shall be in compliance with Data Protection and Payment Card Industry (PCI) standards as contained in sections IV-C and IV-D respectively herein.

B. The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive cardholder data. The PCI Standards defines a series of best practices for handling, transmitting and storing sensitive data.

C. The GraniteCor Retail Showroom shall abide by the Merchant Cards Incident Response Process Flow Chart that is included in section IV-E herein.

D. Inmates working in the GraniteCor Retail Showroom shall not view or touch checks or credit cards.

E. GraniteCor's Retail Showroom shall be as follows:

1. A revenue generating profit center for GraniteCor;
2. A public sales showroom and retail outlet for GraniteCor's products;
3. A place where customers can pick up and pay for pre-ordered GraniteCor made products;
4. A temporary storage place for GraniteCor's raw materials;
5. A GraniteCor administrative and sales office; and

6. A central location for processing checks and credit cards for purchases of products and services.

F. The credit card data is stored on the terminal computer until the bank retrieves it. The bank is responsible for processing the credit card transaction. Once the bank retrieves the credit card transaction, no traceable data remains in the terminal computer. The terminal can be opened by key, which is locked within a key cabinet in the Retail Showroom. No sensitive cardholder data can be accessed by opening the terminal.

G. The staff prints out sales reports from the terminal. The Primary Account Number (PAN) is masked to the last four digits on the print out of the transaction. No other credit card information appears in it. Reports, including copies of the transactions, are transported in a sealed manila envelope to the GraniteCor accounts receivable clerk. Copies of transactions are kept in a locked drawer file cabinet at the GraniteCor Administrative Office. There is no traceable data in these files.

IV. PROCEDURES:

A. Hours of Operation

1. GraniteCor shall strive to keep the Retail Showroom open a minimum of one day a week from 10:00 A.M. to 3:00 P.M. as staffing permits.
2. A state DOC employee shall always be working in the Showroom whenever inmates are present and approved volunteers may work in the Showroom without a state DOC employee present if inmates are not in the Showroom.

B. Sales

1. For all transactions, the credit card holder must be present.
2. Credit Card purchases made at the Retail Showroom for Industries-made purchases less than $25 may be refunded at the Retail Showroom if and only if the product is presented at point of transaction without signs of damage and the owner of the credit card that was used in the original transaction presents the same credit card to the Retail Showroom Clerk. Purchases made by check, or if larger than $25, will not qualify for refund at point of sale and must be processed through a written request for refund that needs approval from the Administrator of Industries.
3. Credit cards and checks used at the Store are to be processed through the processing machine in the customer's presence with the card or check immediately returned to the customer.
4. Cash is not accepted at the Retail Showroom with the following exceptions:
   a. GraniteCor will accept payments outside the Retail Showroom during the Annual Spring and Fall Plant Sale events. Due to the hundreds of $3.00 to $10.00 transactions handled over one or two weeks it is not feasible to process them through the electronic processing machine. Cash will only be accepted for plant sales during the short Spring and Fall events and all sales shall be logged identifying customer, payment type, items purchased, and total payment. Cash will be deposited daily.
   b. Hay sales typically occur when the Retail Showroom is not open. Checks for hay sales will not have to be immediately processed through the electronic processing machine. Address and phone number verification still apply for checks received away from the Showroom.
   c. Firewood sales are collected as it is delivered at the customer's site. Checks for firewood sales will not have to be immediately processed through the electronic processing machine. Address and phone number verification still apply for checks received away from the Showroom.
5. Refunds will not be made without the product being present. If there is a question about the condition of the product, the Shop Manager responsible for making the product may deny the refund or submit a request for refund to the Administrator of Industries for approval. The product will be secured away from the sales floor until the refund has been processed or returned to the buyer if refund is denied.
6. Posters cautioning personnel to safeguard credit card information shall be placed wherever credit card transactions are made or records stored. This will be GraniteCor's formal security awareness program. Posters will be changed at least annually.

7. All staff working in the Retail Showroom shall protect cardholder data. Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Card-member ID (Discover) or CID Card Identification Number (American Express) (e.g., three- or four-digit value printed on the front or back of a payment card).
8. Currently GraniteCor accepts credit cards for transactions at the Retail Showroom. These transactions occur in the stand-alone terminal at the Retail Showroom. The terminal was purchased from First Data Merchants Services (Model FD 2000-telecheck). The customer offers his card to the staff. The staff member inserts the card into the terminal and removes it quickly with a swipe-card movement and returns the card to the customer.
9. All GraniteCor employees assigned to handle credit card transactions will be formally trained to be compliant with Payment Card Industry Data Security Standards (PCI DSS) and in secure handling of credit cardholder data. At the conclusion of the training, attendees will sign off that they have reviewed the instructions and understand the contents. Re-training will take place on an annual basis. New employees assigned to handle credit card transactions will be required to receive training upon hiring, as follows:
   a. Explanation of PCI DSS;
   b. PCI DSS 12 point requirements – information security policy;
   c. Daily operation procedures;
   d. Policies and procedures for data control;
   e. Policies and procedures for protecting cardholder data;
   f. Policies and procedures for data retention and disposal;
   g. Policies and procedures for controlling storage;
   h. Policies and procedures for maintenance of hard copy;
   i. Policies and procedures to manage service providers;
   j. Media destruction policy;
   k. Usage policies for critical employee –facing technologies; and
   l. Policies and procedures in the event of compromised data (breach).
10. Electronic Processing Machines shall be closed out at the end of any day in which they were used.
11. Educational aids include this Policy Manual, posters, Internet, DOIT Merchant Account Blog, and First Data Merchant Services training book.

C. Data Protection

1. Shops within GraniteCor may not negotiate their own contracts with credit card companies, processors, or external services that accept credit card payments on GraniteCor's behalf.
2. Only the Administrator of Industries is authorized to issue GraniteCor bank merchant ID account numbers, which are required for GraniteCor acceptance of credit card payments and to enable deposits through the Chief Financial Officer or CFO's designee.
3. GraniteCor has established contracts, incorporating the necessary security provisions, for any system and service components needed for the acceptance and processing of electronic credit card transactions. If a required service is not already covered by a GraniteCor contract, accounts receivable must work through GraniteCor's Accountant III to identify and contract for approved necessary services and ensure the security of those services.
4. Credit card numbers shall not be transmitted via e-mail or stored in a continual manner on any GraniteCor computer, storage device, or other electronic medium. Any associated paper or other records or reports containing credit card customer information shall be stored in locked cabinets and access shall be limited to only those employees who need this information to accomplish their work.
5. All credit card information is confidential. Whatever information might exist, will be in a locked room and locked file cabinet during non-business hours. The Administrator of Industries must approve all changes in the storage of credit card records.
6. GraniteCor's Accountant III will oversee credit card records and ensure that they will be properly stored for lengths of time required by law and then boxed, sealed, marked as

confidential, and marked for destruction by cross-shredding, pulping, or incinerating. These boxes will be shipped to the Department's warehouse for destruction. The Department's Warehouse Manager will be responsible for the proper safeguarding of these records until destroyed and will oversee the destruction thereafter.

7. Relocation of any transaction records must be approved by the Administrator of Industries.
8. A standard Department Incident Report will be written for any breach of this policy with a copy hand carried to the GraniteCor Administrator.
9. GraniteCor shall follow the Security Incident Response Plan and escalation process as depicted in the Merchant Cards Incident Response Process Flow Chart included in this PPD (Attachment 2).

D. PCI Compliance

1. The point of payment at the Retail Showroom shall guard against exposure or theft of an account in compliance with the Payment Card Industry's Data Security Standards (PCI DSS) requirements for transferring, handling and storage of credit card information.
2. Definition of roles and responsibilities of employees, contractors, service providers are as follows:
    a. The terminal operator:
        1) Operates the terminal on daily basis;
        2) Generates reports;
        3) Interacts with service providers when necessary;
        4) Remains with the service provider during repair to monitor activity; and
        5) Keeps log of any service provider activity.
    b. Telecheck Merchant Service (service provider) is responsible for:
        1) Technical support of software and computer terminal and other technical support; and
        2) Installation of new equipment and terminal repairs.
    c. Contractor is any other service technician responsible for system/terminal as well as repair.
    d. Chief Security Officer (Administrator of Industries, GraniteCor Accountant III), will be responsible for:
        1) Overseeing any staff activity;
        2) Annual checks that security procedures are being followed;
        3) Overseeing staff ongoing required training; and
        4) Maintaining staff compliance with the PCI DSS guidelines.
3. Daily Operational Security Procedures
    a. The assigned staff will swipe credit cards.
    b. All transaction copies (settlement reports) should be checked for traceable data.
    c. The information pulled from the terminal should only reflect the cardholder name, masked PAN, time of purchase, and amount purchased, and total cost.
    d. Security alert will be monitored and information distributed by assigned staff member.
    e. After closing the batch, the staff member will secure and shut down the terminal for the night.
    f. Those who have been granted access to the terminal will complete log sheets of staff activity.
    g. Although there is no traceable data retrieved by GraniteCor staff from the terminal, there is traceable data stored within the terminal until it is retrieved by Telecheck Merchant Card Services (TMCS) on a nightly basis. The policy and procedures listed below address security issues that might arise during any event (breach) as follows:
        1) The Chief Security Officer (Administrator of Industries/Accountant III) will assign the responsibility for creating and distributing security incident response escalation procedures to the staff that operates the terminal.
        2) All users granted access to the terminal would be assigned a unique user name and password.
        3) A list of devices and personnel authorized to use devices will be kept.

4) Acceptable use of technology will be followed, i.e., tracking sales of merchandise.
5) A list of agency-approved technology products will be used, i.e., Model FD 220-Telecheck.
6) Remote access sessions will be prohibited to anyone.
7) All service providers will be prohibited from copying, moving or storing of cardholder data onto local hard drive and removable electronic media.
8) Policies and Procedures for Data Control:
    a) GraniteCor is compliant with the PCI DSS standard that requires access rights for privileged users to be restricted with the least privileges necessary to perform job responsibilities. Designated staff will access the terminal with user id and password. Once they have access they are viewing non-traceable data only.
    b) Any GraniteCor employee granted access to the FD 200 Terminal will be based on job description and assigned roles/responsibilities.
    c) A formal authorization form (verification of training and completion of this manual on page 27) will be issued by the Administrator of Industries to assigned employees. This document will be signed by both the Administrator of Industries and employee assigned access to any data, even though the data is considered non-traceable.
9) Policies for Protecting Cardholder Data:
    a) Control procedure for physically securing electronic data is as follows:
        i. The data retrieved from the terminal by the staff member is not traceable.
        ii. The traceable data is retrieved only by Telecheck Merchant Services (TMCS) on a daily basis.
        iii. Any agreement as outlined for both terminal and access to sensitive cardholder data within the terminal computer will be stored with other PCI DSS materials.
    b) Control procedures for physically securing paper reports (hard copy) is as follows:
        i. The reports generated include monthly sales report and daily sales supplemental report.
        ii. The list of the detailed transactions printed from the computer does not include sensitive data.
        iii. The PAN is masked to the last four digits.
        iv. There is no expiration date, PIN number, or magnetic strip information.
        v. The only information displayed on paper copies is the cardholder name, masked PAN, time and amount of sales.
    c) Despite the lack of traceable data, precautions are taken by locking all reports in a file cabinet located at the Retail Showroom. Reports are sent to the Accounts Receivable clerk at the GraniteCor administrative office in a sealed manila envelope for transportation.
    d) There is no distribution of cardholder data media.
    e) The PCI DSS requirement demanding that all media must be classified as confidential does not apply to GraniteCor credit card transaction detail as this data is non-traceable.
    f) No media containing sensitive cardholder data is transported outside the GraniteCor facility.
    g) The Administrator of Industries will sign off on any log for the movement of any and all sensitive media should the situation arise.
10) Policies and procedures for encrypted transmission of cardholder data across public networks:
    a) No unencrypted cardholder data is ever transmitted over open networks such as the web, e-mail, instant message, or chat.

b) Telecheck Merchant Service retrieves sensitive cardholder data via a modem/dedicated phone line every 24 hours. Once this retrieval is complete, no traceable data remains on the terminal computer until the next sales transaction occurs.

11) Policies and procedures for data retention and disposal:
  a) Hard paper copies of reports do not contain traceable data. The PAN is masked with only the last four digits and cardholder name. There is no visible expiration date, PIN number, or other sensitive data. Despite the non-traceable nature of the data, all current reports will be cross-cut shredded at the end of the storage date. The hard copies will be stored for a period that satisfies State of NH audit requirements on financial data and destroyed after the designated period.
  b) The Administrator of Industries will be responsible for the creation and distribution of a formal security incident response as well as procedures in the event of escalation.
  c) The Administrator of Industries will require an annual inventory and review of hard copy and hardcopy data as well as the flow of sensitive traceable data from the terminal to Telecheck Merchant Services. Compliance will be checked for any service providers granted access to sensitive data. No electronic media is stored within the GraniteCor system, and an annual PCI audit shall be performed.

12) Policies and procedures to manage service providers:
  a) Telecheck Merchant Services will be the sole service provider.
  b) The CFO will approve a formal agreement written by the GraniteCor Administrator of Industries should any service provider have access to the sensitive cardholder data. This agreement to be signed by all GraniteCor service providers will be their acknowledgement of responsibility for security of all sensitive cardholder data accessed. In addition to the agreement, all activity will be logged and monitored (Attachment 1).
  c) All service providers will be required to submit proof of PCI DSS compliance. All future providers will be required to provide proof of PCI DSS compliance with a short procedural document in their handling of credit card data or verification from a qualified security assessor that they are PCI DSS compliant.

13) Media destruction policy:
  a) Currently there is no electronic media containing sensitive cardholder data. In the event data retention is necessary, all media would be erased utilizing approved over-write or media swipe software and all activity logged.
  b) Hard copies (reports) do not contain traceable data but are cross-cut shredded as a matter of procedure after the required amount of storage time mandated by the State of NH.
  c) GraniteCor does not store sensitive cardholder data electronically. Should the situation change, all electronic media will be rendered unrecoverable by the GraniteCor security officer.

E. <u>Incident Response Plan in the event of Compromise & Escalation</u>

1. Telecheck Merchant Services will notify GraniteCor in the event of compromise as they are the only entity handling sensitive cardholder data and would be the first to recognize a compromise/breach.
2. Upon notification by Telecheck Merchant Services of the breach, the staff assigned to operate the terminals will immediately shut down both terminals until further notice.
3. The Administrator of Industries will be informed of the breach, and will in turn inform the Office of the Commissioner.

4. All instruction provided by Telecheck Merchant Services will be followed explicitly and all actions will be logged until resolution is achieved. GraniteCor staff will keep an open line of communication with Telecheck Merchant Services and will log all activity until resolution is achieved.
5. Procedures will be analyzed to examine the cause of the compromise. Action will be taken to prevent a future compromised situation.
6. Once all parties are satisfied that business can resume without the possibility of future compromise, business will resume with new procedures and policies in place.
7. The Administrator of Industries will attend to compliance with R.S.A. 359-C:19, 20, 21, in the event of an incident. RSA 359-C:19, 20, 21 basically states that in the event of a breach of computer security, GraniteCor will notify all private parties who are or may be affected; notify any government agency which regulates the business being conducted, or the Attorney General's Office if no other government agency has jurisdiction (See Attachment 3, pp 24-25).
8. The Administrator of Industries will conduct an annual test of the incident response plan.
9. GraniteCor will observe the subsequent State's Merchant Cards Incident Response Process as described in the flow chart (Attachment 2).

REFERENCES:

Standards for the Administration of Correctional Agencies
Second Edition Standards

Standards for Adult Community Residential Services
Fourth Edition Standards

Other

Standards for Adult Correctional Institutions
Fourth Edition Standards

Standards for Adult Probation and Parole Field Services
Third Edition Standards

McGonagle/pf

Attachments

Attachment 1

****Service Provider Log Sheet Terminal Activity Log***

Service Provider/Name	Activity	Time In	Time Out

The following is the designated PCI DSS Information Security Policy

If a suspected security breach occurs, the payment brand procedures must be followed. They are found as follows: (A) MasterCard Security Rules and Procedures, Section 10, Account Data Protection Standards and Programs, Account Data Compromise User Guide – these are available on the MasterCard website; (B) Visa, What to do If Compromised – this is available on the Visa website; (C) Discover Card, Data Security Breach Section – this is available on the Discover website; (D) American Express, Data Security Operating Policy – this is available on the American Express website.

Information Security Policy

This set of policies and procedures addresses all 12 PCI DSS requirements, including administrative and technical procedures for each of the requirements. These policies and procedures are consistent with PCI DSS Requirement 12.

PCI DSS Requirement 1 – Install and maintain a firewall configuration to protect Cardholder data

- Req. 1.1 – Non-traceable data is retrieved from the terminals. These terminals are not connected to any computer system in GraniteCor or elsewhere. No data is transmitted electronically from these terminals. Sensitive cardholder data is transmitted through dedicated phone lines to Telechek Merchant Services.
    - ➢ Req. 1.1.1 – Approve and test all external network connections and changes to the firewall and router configurations. All tests to be performed by the TMCS, GraniteCor Administrator of Industries, on a quarterly basis.
    - ➢ Req. 1.1.2 – Provide current network diagram with all connections cardholder data, including wireless network. The TMSC, SCO will create this diagram.
    - ➢ Req. 1.1.3 – Requirement for firewalls at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. Sensitive cardholder data is not transmitted over the Internet.
    - ➢ Req. 1.1.4 – Requirement to define groups, roles and responsibilities for logical management of network components. There are only two designated employees as well as the Administrator of Industries involved with this process. The Administrator of Industries is responsible for overseeing all activity. The terminal operator handles all technical aspects of the handling of such transaction, and is assigned the responsibility of day to day operations, reports and monitoring the system.
    - ➢ Req. 1.1.5 – Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. No transmission of sensitive data other than the retrieval by Telecheck Merchant Services who is PCI DSS compliant.
    - ➢ Req. 1.1.6 – Requirement to review firewall and router rule sets at least every six months. No sensitive data is transmitted by GraniteCor.
- Req. 1.2 - Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment not networked to any system. Precautionary firewalls are in place.
    - ➢ Req. 1.2.1 – Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. No traffic exists other than the Telecheck Merchant Services retrieval of data.
    - ➢ Req. 1.2.2 – Secure and synchronize router configuration files via dedicated modem line.
    - ➢ Req. 1.2.3 – Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless

environment or to control any traffic (if such traffic is necessary for business purposes). Non-applicable: Sensitive cardholder data not stored on computer.

- Req. 1.3 – Prohibit direct public access between the internet and any system component in the cardholder data environment. Non-applicable: No cardholder data accepted via internet.
  - ➢ Req. 1.3.1 – Implement a DMZ to limit inbound and outbound traffic to any protocols that are necessary for the cardholder environment. Sensitive data only accessible through dedicated modem line by Telecheck Merchant Services.
  - ➢ Req. 1.3.2 – Limit inbound internet traffic to IP addresses within the DMZ zone. Non-applicable: No inbound internet traffic
  - ➢ Req. 1.3.4 – No internal addresses will be allowed to pass from the internet to the DMZ. Non- applicable: No inbound internet traffic.
  - ➢ Req. 1.3.5 – Restrict outbound traffic from the cardholder data environment to the internet such that outbound traffic can only access IP addresses within the DMZ. Non-applicable: Outbound cardholder data transmitted only through dedicated phone line.
  - ➢ Req. 1.3.6 – Implement stateful inspection, also known as dynamic packet filtering (only established connections allowed into the network). No data stored.
  - ➢ Req. 1.3.7 – Place the database in an internal network zone, segregated from the DMZ. Non-applicable: No data stored.
  - ➢ Req. 1.3.8 – Implement IP masquerading to prevent internal addresses from being translated and revealed on the internet using RFC 1918 address space. Non-applicable: No data stored.
- Req. 1.4 – Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the internet (for example computers with direct connectivity to the internet (for example, laptops used by employees) which are used to access the organization's network. Non applicable: No data stored.

Requirement 2 – Do not use vendor supplied defaults for system passwords and other security parameters

- Req. 2.1 - Always change vendor-supplied defaults before installing a system on the network (i.e. include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts). All defaults changed during installation on ___________. Non applicable: Not networked.
  - ➢ Req. 2.1.1 – For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission. Non-applicable: No wireless
- Req. 2.2 – Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Non-applicable: Password protected, no sensitive data.
  - ➢ Req. 2.2.1 – Implement only one primary function per server. Non-applicable: Not networked to server.
  - ➢ Req. 2.2.2 – Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function). Non-applicable: but also were disabled.
  - ➢ Req. 2.2.3 – Configure system security parameters to prevent misuse. Non-applicable: Password protected.
  - ➢ Req. 2.2.4 – Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers. Non-applicable: Not connected to web
- Req. 2.3 – Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative services. Non-applicable: No web based application.

- Req. 2.4 – Shared hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in "Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers." Non-applicable: No shared hosting.

Requirement 3 – Protect Cardholder Data

- Req. 3.1 – Keep cardholder data storage to a minimum. No sensitive cardholder data is stored. Only reports reflecting a masked PAN are stored. State of NH guidelines for storage of financial data are met. Once the time period has passed, reports are destroyed appropriately.
- Req. 3.2 – Do not store sensitive authentication data after authorization. Sensitive data is overwritten after retrieval by Telecheck Merchant Card Service.
  - Req. 3.2.1 – Do not store the full contents of any track from the magnetic stripe (full track). Non-applicable: GraniteCor does not have access to this sensitive data.
  - Req. 3.2.2 – Do not store the card-validation code or value (3 or 4 digit printed on the front or back of payment card) used to verify card not present transactions. Non-applicable: GraniteCor does not have access to this sensitive data.
  - Req. 3.2.3 – Do not store the personal identification number (PIN) or the encrypted PIN block. Non-applicable: GraniteCor does not have access to this sensitive data.
- Req. 3.3 – Mask PAN when displayed. All PANs are masked except for the last four digits on display, receipt and reports.
- Req. 3.4 – Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs) by using any of the following approaches: one-way hashes based on strong cryptography; truncation; index tokens and pads or strong cryptography with associated key management processes and procedures. Non-applicable:
  - Req. 3.4.1 – If disk encryption is used (rather than file-or-column database encryption) logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tiered to user accounts. Non-applicable:
- Req. 3.5 – Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse. Non-applicable:
  - Req. 3.5.1 – Restrict access to cryptographic keys to the fewest number of custodians necessary. Non-applicable:
  - Req. 3.5.2 – Store cryptographic keys securely in the fewest locations and forms. Non-applicable:
- Req. 3.6 – Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:
  - 3.6.1 – Generation of strong cryptographic keys
  - 3.6.2 – Secure cryptographic key distribution
  - 3.6.3 – Secure cryptographic key storage
  - 3.6.4 – Periodic cryptographic key changes
  - 3.6.5 – Retirement or replacement of old or suspected compromised cryptographic keys
  - 3.6.6 – Split knowledge and establishment of dual control of cryptographic keys
  - 3.6.7 – Prevention of unauthorized substitution of cryptographic keys\
  - 3.6.8 – Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities
  - None of the above is applicable:

Requirement 4 – Encrypt transmission of cardholder data across open public networks. No open public network transmission

- Req. 4.1 – Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks (internet, wireless technologies, global system for mobile communications (GSM) and general packet radio service (GPRS)). Non-applicable:

  - Req. 4.1.1 – Ensure wireless networks transmitting cardholder data or connected to the cardholder to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Non-applicable:
- Req. 4.2 – Never send unencrypted PANs by user-end messaging technologies (for example, email, instant messaging, chat). All PANs are masked and are never send via email, instant messaging, chat etc.

Requirement 5 – Use and regularly update anti-virus software or program. Non applicable: Updates are performed on a regular basis by the Security Officer or the designated employee.

- Req. 5.1 – Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). Data stored on the computer is not trackable data. The computer is not connected to a network or server at this time. As a matter of course, anti-virus software is updated and monitored by the Security Officer.
  - Req. 5.1.1 – Ensure that all anti-virus programs are capable of detecting, removing and protecting against all known types of malicious software as outlined above.
- Req. 5.2 – Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs designated to the Security Officer.

Requirement 6 – Develop and maintain secure systems and application If action is required, it is performed by GraniteCor Administrator.

- Req. 6.1 – Ensure that all system components and software have the latest vendor supplied security patches installed. Install critical security patches within one month of release. Non-applicable:
- Req. 6.2 – Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues. This is performed as a matter of course by GraniteCor Administrator.
- Req. 6.3 – Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development cycle. These processes must include the following:
  - Req. 6.3.1 - Testing of all security patches, and system and software configuration changes before deployment.
    - Req. 6.3.1.1 – Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.
    - Req. 6.3.1.2 – Validation of proper error handling
    - Req. 6.3.1.3 – Validation of secure cryptographic storage
    - Req. 6.3.1.4 – Validation of secure communication
    - Req. 6.3.1.5 – Validation of proper role-based access control (RBAC)
    - Non-applicable:
  - Req. 6.3.2 – Separate development/test and production environments. Non-applicable:
  - Req. 6.3.3 – Separation of duties between development/test and production environments. Non-applicable:
  - Req. 6.3.4 – Production data (live PANs) are not used for testing or development. Non-applicable:
  - Req. 6.3.5 – Removal of test data and accounts before production systems become active. Non-applicable:
  - Req. 6.3.6 – Removal of custom application accounts, user IDs and passwords before applications become active or are released to customers. Non-applicable:
  - Req. 6.3.7 – Review of custom code prior to release to production of customers in order to identify any potential coding vulnerability. Non-applicable:

- Req. 6.4 – Follow change control procedures for all changes to system components. The procedures must include the following:
  - Req. 6.4.1 – Documentation of impact
  - Req. 6.4.2 – Management sign-off by appropriate parties
  - Req. 6.4.3 – Testing of operational functionality
  - Req. 6.4.4 – Back out procedure Non-applicable:
- Req. 6.5 – Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following:
  - Req. 6.5.1 – Cross site scripting (XSS)
  - Req. 6.5.2 – Injection flaws, particularly SQL injection. Also consider LDAP and X-path injection flaws as well as other injection flaws
  - Req. 6.5.3 – Malicious file execution
  - Req. 6.5.4 – Insecure direct object references
  - Req. 6.5.5 – Cross site request forgery (CSRF)
  - Req. 6.5.6 – Information leakage and improper error handling
  - Req. 6.5.7 – Broken authentication and session management
  - Req. 6.5.8 – Insecure cryptographic storage
  - Req. 6.5.9 – Insecure communications
  - Req. 6.5.10 – Failure to restrict URL access Non-applicable:
- Req. 6.6 – For public-facing web applications, address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks by either of the following methods:
  - Reviewing public facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes;
  - Installing a web-application firewall in front of public-facing web applications. Non-applicable:

Requirement 7 – Restrict access to cardholder data by business need-to-know rules and responsibilities. The State employees that touch a customer's check or credit card are limited to those that have signed off on having required training and are currently limited to: Administrator, Sales Associate, the two Logistics staff members, Accountant III, Account Clerk II, and Upholstery Shop Supervisor when attending Expos These designated employees **do not** have access to traceable data.

- Req. 7.1 – Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:
  - Req. 7.1.1 – Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
  - Req. 7.1.2 – Assignment of privileges is based on individual personnel's job classification and function
  - Req. 7.1.3 – Requirement for an authorization form signed by management that specifies required privileges
  - Req. 7.1.4 – Implementation of an automated access control system is addressed under Requirement 7
- Req. 7.2 – Establish a mechanism for system components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following:
  - Req. 7.2.1 – Coverage of all system components
  - Req. 7.2.2 – Assignment of privileges to individuals based on job classification and function
  - Req. 7.2.3 – Default "deny all" setting

Requirement 8: Assign a unique ID to each person with computer access

- Req. 8.1 – Assign all users a unique ID before allowing them access to system components or cardholder data. No GraniteCor employee has access to trackable cardholder data but as a matter of course, user IDs have been assigned to access the one terminal at the Retail Showroom.
- Req. 8.2 – In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
  - Password or passphrase
  - Two-factor authentication (for example, token devices, smart cards, biometrics or public keys Non-applicable: see 8.1
- Req. 8.3 – Incorporate two-factor authentication for remote access (network level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. Non-applicable: see 8.1
- Req. 8.4 – Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms). Non-applicable:
- Req. 8.5 – Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
  - Req. 8.5.1 – Control addition, deletion and modification of user IDs, credentials and other identifier objects
  - Req. 8.5.2 – Verify user identity before performing password resets
  - Req. 8.5.3 – Set first-time passwords to a unique value for each user and change immediately after the first use
  - Req. 8.5.4 – Immediately revoke access for any terminated users.
  - Req. 8.5.5 – Remove/disable inactive user accounts at least every 90 days
  - Req. 8.5.6 – Enable accounts used by vendors for remote maintenance only during the time period needed
  - Req. 8.5.7 – Communicate password procedures and policies to all users who have access to cardholder data
  - Req. 8.5.8 – Do not use group, shared or generic accounts or passwords
  - Req. 8.5.9 – Change user passwords at least every 90 days
  - Req. 8.5.10 – Require a minimum password length of at least 7 characters
  - Req. 8.5.11 – Use passwords containing both numeric and alphabetic characters
  - Req. 8.5.12 – Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she may have used
  - Req. 8.5.13 – Limited repeated access attempts by locking out the user ID after not more than 6 attempts
  - Req. 8.5.14 – Set the lock out duration to a minimum of 30 minutes or until the Administrator enables the user ID
  - Req. 8.5.15 – If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
  - Req. 8.5.16 – Authenticate all access to any database containing cardholder data. This includes access by applications, administrators and all other users. Non-applicable: Passwords are used.

Requirement 9: Restrict physical access to cardholder data

- Req. 9.1 – Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. No physical access unless monitored by designated GraniteCor staff.

- Req. 9.1.1 – Use video cameras or other access control mechanisms to monitor individual access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. The Retail Showroom is patrolled by Correction Officers on a regular basis. The Retail Showroom is locked when not occupied by approved staff. Video cameras are not used in the Retail Showroom.
- Req. 9.1.2 – Restrict physical access to publicly accessible network jacks. Staff has no access.
- Req. 9.1.3 – Restrict physical access to wireless access points, gateways, and handheld devices. Staff has no access.
- Req. 9.2 – Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. Staff wears DOC ID Badge.

- Req. 9.3 – Make sure all visitors are handled as follows:
  - Req. 9.3.1 – Authorized before entering areas where cardholder data is processed or maintained
  - Req. 9.3.2 – Given a physical token (for example, a badge or access device that expires and that identifies the visitors as non-employees
  - Req. 9.3.3 – Asked to surrender the physical token before leaving the facility or at the date of expiration. Non-applicable: No physical access to terminal without key to Retail Showroom
- Req. 9.4 – Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented and the employee authorizing physical access on the log. Retain the log for a minimum of three months, unless otherwise restricted by law. There is no visitor access. Service provider activity logged and monitored (See pg 7).

- Req. 9.5 – Store media backups in a secure location, preferably in an off-site facility, such as an alternate or back-up site, or commercial storage facility. Review the location's security at least annually. Sensitive traceable data is not stored.
- Req. 9.6 – Physically secure all paper and electronic media that contains cardholder data. Non-applicable:
- Req. 9.7 – Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:
  - Req. 9.7.1 – Classify the media so it can be identified as confidential
  - Req. 9.7.2 – Send the media by secured courier or other delivery method that can be accurately tracked. Non-applicable:
- Req. 9.8 – Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals) Non-applicable:
- Req. 9.9 – Maintain strict control over the storage and accessibility to media that contains cardholder data. Non-applicable:
  - Req. 9.9.1 – Properly maintain inventory logs of all media and conduct media inventories at least annually. Non-applicable:
- Req. 9.10 – Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:
  - Req. 9.10.1 – Shred, incinerate or pulp hardcopy materials so that cardholder data cannot be reconstructed
  - Req. 9.10.2 – Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed

Requirement 10: Track and monitor all access to network resources and cardholder Data

- Req. 10.1 – Establish a process for linking all access system components (especially access done with administrative privileges such as root) to each individual user. Non-applicable:

- Req. 10.2 – Implement automated audit trails for all system components to reconstruct the following events:
  - Req. 10.2.1 – All individual user accesses to cardholder data
  - Req. 10.2.2 – All actions taken by any individual with root or administrative privileges
  - Req. 10.2.3 – Access to all audit trails
  - Req. 10.2.4 – Invalid logical access attempts
  - Req. 10.2.5 – Use of identification and authentication mechanisms
  - Req. 10.2.6 – Initialization of the audit logs
  - Req. 10.2.7 – Creation and deletion of system-level objects
  - Non-applicable: Performed by Telcheck Merchant Card Services
- Req. 10.3 – Record at least the following audit trail entries for all system components for each event
  - Req. 10.3.1 – User identification
  - Req. 10.3.2 – Type of event
  - Req. 10.3.3 – Date and time
  - Req. 10.3.4 – Success or failure indication
  - Req. 10.3.5 – Origination of event
  - Req. 10.3.6 – Identify or name of affected data, system component or resource. Non-applicable:
- Req. 10.4 – Synchronize all critical system clocks and times.
- Req. 10.5 – Secure audit trails so they cannot be altered. Non-applicable:
  - Req. 10.5.1 – Limit viewing of audit trails to those with a job-related need. Non-applicable:
  - Req. 10.5.2 – Protect audit trail files from unauthorized modifications. Non-applicable:
  - Req. 10.5.3 – Promptly back up audit trail files to a centralized log server or media that is difficult to alter. Non-applicable:
  - Req. 10.5.4 – Write logs for external-facing technologies onto a log server on the internal LAN. Non-applicable:
  - Req. 10.5.5 – Use file-integrity monitoring and change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) Non-applicable:
- Req. 10.6 – Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization and accounting protocol (AAA) servers (for example, RADIUS). Non-applicable:
- Req. 10.7 – Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived or restorable from back-up). Non-applicable:

Requirement 11: Regularly test security systems and processes

- Req. 11.1 – Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. Non-applicable:
- Req. 11.2 – Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). Non-applicable:
- Req. 11.3 – Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment or a web server added to the environment). These penetration tests must include the following:
  - Req. 11.3.1 – Network-layer penetration tests
  - Req. 11.3.2 – Application-layer penetration tests Non-applicable:

- Req. 11.4 – Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date. Non-applicable:
- Req. 11.5 – Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files and configure the software to perform critical file comparisons at least weekly. Non-applicable:

Requirement 12: Maintain an Information Security Policy

- Req. 12.1 Establish, publish, maintain and disseminate a security policy that accomplishes the following:
  - Req. 12.1.1 – Addresses all PCI DSS requirements
  - Req. 12.1.2 – Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment
  - Req. 12.1.3 – Includes a review at least once a year and updates when the environment changes
  - To be performed by GraniteCor Administrator and Retail Showroom staff person.
  - Req. 12.2 – Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures and log review procedures).
- Req. 12.3 – Develop usage policies for critical employee-facing technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email usage and internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:
  - Req. 12.3.1 – Explicit management approval
  - Req. 12.3.2 – Authentication for use of the technology
  - Req. 12.3.3 – List of all such devices and personnel with access
  - Req. 12.3.4 – Labeling of all such devices and personnel with access
  - Req. 12.3.5 – Acceptable uses of the technologies
  - Req. 12.3.6 – Acceptable network locations for the technologies
  - Req. 12.3.7 – List of company-approved products
  - Req. 12.3.8 – Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
  - Req. 12.3.9 – Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use
  - Req. 12.3.10 – When accessing cardholder data remotely via remote-access technologies, prohibit, copy, move, and storage of cardholder data onto local hard drives and removable electronic media. These requirements are covered under the previous sections. Please refer to the Protecting Cardholder Data section.
- Req. 12.4 – Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors. These requirements are met and covered in the GraniteCor manual sections, “Operational Procedures,” “Critical Employee-Facing Technologies,” and “Procedure for Data Control.”
- Req. 12.5 – Assign to an individual or team information security management responsibilities as follows:
  - Req. 12.5.1 – Establish, document and distribute security policies and procedures.
  - Req. 12.5.2 – Monitor and analyze security alerts and information, and distribute to appropriate personnel
  - Req. 12.5.3 – Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
  - Req. 12.5.4 – Administer user accounts, including additions, deletions and modification

  - Req. 12.5.5 – Monitor and control all access to data
  - These requirements are met and covered in the GraniteCor manual sections, "Operational Procedures," "Critical Employee-Facing Technologies," and "Procedure for Data Control."
- Req. 12.6 – Implement a formal security awareness program to make all employees aware of the importance of cardholder data security
  - Req. 12.6.1 – Educate employees upon hire and at least annually
  - Req. 12.6.2 – Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures
  - Requirement 12.6 has been met and is covered by the Formal Security Awareness Training Section of this manual
- Req. 12.7 – Screen potential employees prior to hire to minimize the risk of attacks from internal sources. GraniteCor employees do not have access to critical cardholder data.
- Req. 12.8 – If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:
  - Req. 12.8.1 – Maintain a list of service providers
  - Req. 12.8.2 – Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess
  - Req. 12.8.3 – Ensure there is an established process for engaging service providers including proper due diligence prior to engagement
  - Req. 12.8.4 – Maintain a program to monitor service providers' PCI DSS compliance status
  - These requirements are met and covered in the "Managing Service Providers" section of this manual
- Req. 12.9 – Implement an incident response plan. Be prepared to respond immediately to a system breach.
  - Req. 12.9.1 – Create the incident response plan to be implemented in the event of a system breach. Ensure the plan addresses the following, at a minimum:
    - Roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of the payment.
    - Specific incident response procedures
    - Business recovery and continuity procedures
    - Data back-up processes
    - Analysis of legal requirements for reporting compromises
    - Coverage and responses of all critical system components
    - Reference or inclusion of incident response procedures from the payment brands
    - These requirements are met. Please refer to Incident Response Section of this manual.
  - Req. 12.9.2 – Test the plan annually
  - Req. 12.9.3 – Designate specific personnel to be available on 24/7 basis to respond to alerts
  - Req. 12.9.4 – Provide appropriate training to staff with security breach response responsibilities
  - Req. 12.9.5 – Include alerts from intrusion-detection, intrusion-prevention, and file integrity monitoring systems.
  - Req. 12.9.6 – Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
  - These requirements are met and detailed in the Incident Response Section of this manual. (See page 8).

Notice of Security Breach

Section 359-C:19

359-C:19 Definitions. – In this subdivision:

I. ""Computerized data" means personal information stored in an electronic format.

II. ""Encrypted" means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall not be considered to be encrypted for purposes of this subdivision if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data.

III. ""Person" means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state.

IV. (a) ""Personal information" means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or other government identification number.

(3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(b) ""Personal information" shall not include information that is lawfully made available to the general public from federal, state, or local government records.

V. ""Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Source. 2006, 242:1, eff. Jan. 1, 2007.

Section 359-C:20

359-C:20 Notification of Security Breach Required. –

I. (a) Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.

(b) Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office the names of the individuals entitled to receive the notice or any personal information relating to them. The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section.

(c) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.

II. Notification pursuant to paragraph I may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.

III. The notice required under this section shall be provided by one of the following methods:

(a) Written notice.

(b) Electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means.

(c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons.

(d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to subparagraphs I(a)-I(c). Substitute notice shall consist of all of the following:

(1) E-mail notice when the person has an e-mail address for the affected individuals.

(2) Conspicuous posting of the notice on the person's business website, if the person maintains one.

(3) Notification to major statewide media.

(e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information.

IV. Notice under this section shall include at a minimum:

(a) A description of the incident in general terms.

(b) The approximate date of breach.

(c) The type of personal information obtained as a result of the security breach.

(d) The telephonic contact information of the person subject to this section.

V. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidance, or guidelines issued by a state or federal regulator shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidance, or guidelines.

VI. (a) If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p), of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.

(b) Subparagraph (a) shall not apply to a person who is subject to Title V of the Gramm, Leach-Bliley Act, 15 U.S.C. section 6801 et seq.

Source. 2006, 242:1, eff. Jan. 1, 2007.

Section 359-C:21

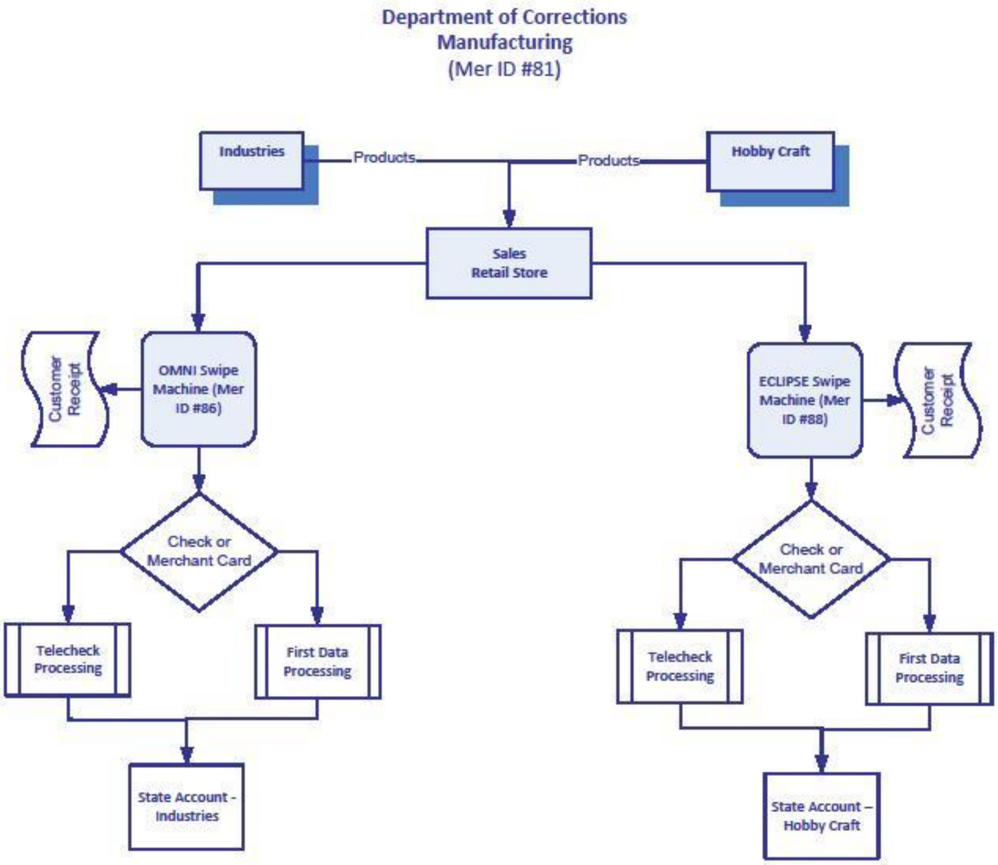
359-C:21 Violation. –

I. Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph shall be void and unenforceable. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court.

II. The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4.

III. The burden shall be on the person responsible for the determination under RSA 359-C:20, I to demonstrate compliance with this subdivision.

Source. 2006, 242:1, eff. Jan. 1, 2007



PCI DSS STAFF TRAINING VERIFICATION SHEET

GraniteCor staff training verification: I have read this manual in its entirety as well as PCI DSS materials. I understand the content of this manual and will comply with all PCI DSS requirements.

Employee's Signature Date

Administrator's Signature Date

Employee's Signature Date

Administrator's Signature Date

Employee's Signature Date

Administrator's Signature Date

Employee's Signature Date

Administrator's Signature Date