Credit Card (PCI) Security Incident Response Plan

To address credit cardholder security, the major credit card brands (Visa, MasterCard, American Express, Discover) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create and document an incident response plan. The Granite City Food and Brewery PCI Security Incident Response Team (PCI Response Team) is comprised of the IT Director, IT support staff, and the VP of Finance.

1. The person who discovers the incident will call the IT support number at 952-215-0677. Incidents may be discovered by and are required to be reported by:
    1. IT Support Staff
    2. 3rd party firewall services Secured Retail
    3. 3rd party firewall services Vendor Safe
    4. 3rd Party POS vendor: Foremost Business Systems Inc.
    5. 3rd Party POS vendor: NCR
    6. Internal Store Management

    All parties listed above will receive contact information and a copy of the SIRP on at least an annual basis or whenever it updated.

2. If the person discovering the incident is a member of the IT department, they will proceed to step 5.
3. If the person discovering the incident is not a member of the IT department or affected department, they will call the 24/7 reachable IT Support Line 952-215-0677.
4. The On-call IT support team member will log:
    1. The name of the caller.
    2. Time of the call.
    3. Contact information about the caller.
    4. The nature of the incident.
    5. What equipment or persons are involved.
    6. Location of equipment or persons involved.
    7. How was the incident detected?
    8. When was an event first noticed that supported the idea that the incident occurred?
    9. Is the equipment affected business critical?
    10. What is the severity of the potential impact?

11. Name of system being targeted, along with operating system, IP address, and location.
12. IP address and any information about the origin of the attack.

5. The IT staff member who receives the call (or discovered the incident) shall refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will be sure the IT Director is contacted using both email and phone messages while being sure other appropriate and backup personnel and managers designated are contacted.

Contact list includes:

Don Stegman	Director MIS/IT	612-819-2393	dstegman@gcfb.net
David Regal	Lead IT Specialist	651-280-9288	dregal@gcfb.net
Greg Neutz	IT Support Technician	612-723-8771	gneutz@gcfb.net
Jeff Romness	IT Support Technician	952-388-3982	jromness@gcfb.net
Monica Underwood	VP of Finance	952-215-0662	munderwood@gcfb.net
Jeff Rager	CFO	832.655.1481	jrager@gcfb.net

6. Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
    1. Is the incident real or perceived?
    2. Is the incident still in progress?
    3. What data or property is threatened and how critical is it?
    4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    5. What system or systems are targeted, where are they located physically and on the network?
    6. Is the incident inside the trusted network?
    7. Is the response urgent?
    8. Can the incident be quickly contained?
    9. Will the response alert the attacker and do we care?
    10. What type of incident is this? Ex: virus, worm, intrusion, abuse, damage.
7. An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

1. Category one - A threat to public safety or life.
2. Category two - A threat to sensitive data
3. Category three - A threat to computer systems
4. Category four - A disruption of services

If a breach is confirmed the IT Director will reach out to the following:

American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750/US only, or at 1-(602) 537-3021/International, or email at EIRP@aexp.com.

VISA Fraud Control (650) 432-2978 or usfraudcontrol@visa.com

MasterCard compromised account team 1-636-722-4100
compromised_account_team@mastercard.com

Vantiv: Heather Huddleston | Merchant Relationship Manager P&F: 513.900.3732
heather.huddleston@ftpsllc.com and the Vantiv Helpdesk: HD: 877.744.5300 |

8. In response to a systems compromise, the PCI Response Team will:
   1. Ensure compromised system/s is isolated on/from the network.
   2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls
   3. Conduct appropriate forensic analysis of compromised system.
   4. Contact internal and external departments and entities as appropriate.
   5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
   6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

9. Team members will use forensic techniques including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized people should be performing interviews or examining evidence and the authorized personnel may vary by situation and the organization.
10. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

11. Upon management approval, the changes will be implemented.
12. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    1. Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    2. Make users change passwords if passwords may have been sniffed.
    3. Be sure the system has been hardened by turning off or uninstalling unused services.
    4. Be sure the system is fully patched.
    5. Be sure real time virus protection and intrusion detection is running.
    6. Be sure the system is logging the correct events and to the proper level.
13. Documentation - The following shall be documented:
    1. How the incident was discovered.
    2. The category of the incident.
    3. How the incident occurred whether through email, through firewall, etc.
    4. Where the attack came from such as IP addresses and other related information about the attacker.
    5. What the response plan was.
    6. What was done to respond?
    7. Whether the response was effective.
14. Evidence Preservation - Make copies of logs, email, and other documentable communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
15. Notify proper external agencies -
16. Assess damage and cost - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
17. Review response and update policies - Plan and take preventative steps so the intrusion can't happen again.
    1. Consider whether an additional policy could have prevented the intrusion.
    2. Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
    3. Was the incident response appropriate? How could it be improved?
    4. Was every appropriate party informed in a timely manner?
    5. Were the incident response procedures detailed and cover the entire situation? How can they be improved?
    6. Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    7. Have changes been made to prevent a new and similar infection?

8. Should any security policies be updated?
9. What lessons have been learned from this experience?