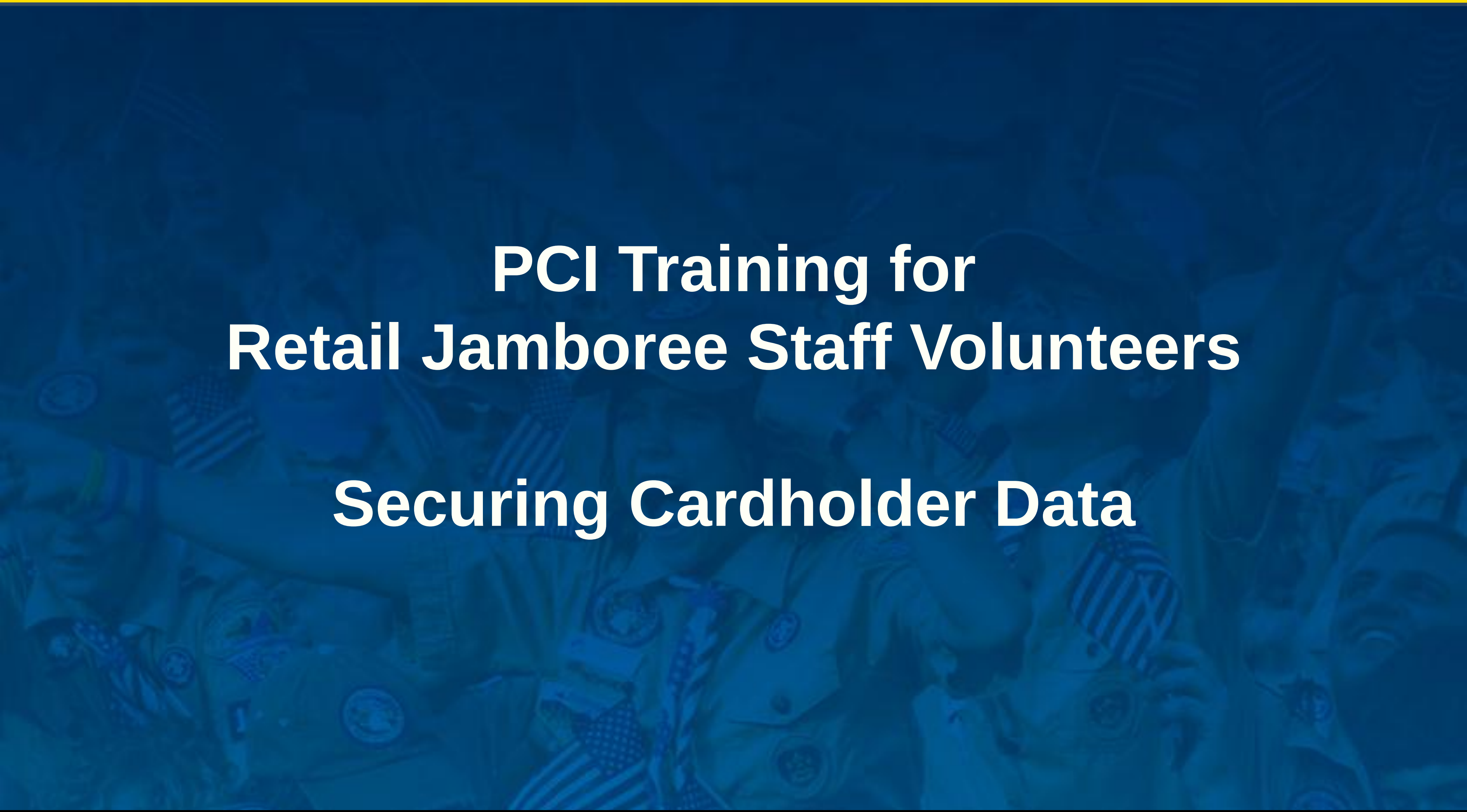


PCI Training for
Retail Jamboree Staff Volunteers

Securing Cardholder Data

Securing Cardholder Data – Introduction

This PowerPoint presentation is designed to educate Retail Jamboree Staff volunteers on what security measures must be taken to protect the private information of individuals during any transaction occurring with the use of a credit card (e.g., Visa, MasterCard, etc.) Throughout this course, we will refer to the Payment Card Industry as PCI and the Payment Card Industry Data Security Standard as PCI DSS. This standard is used by all card brands to ensure the security of the cardholder data related to credit, debit and electronic payment cards.

This course includes terms you may need to know, your responsibilities, vulnerabilities of which you should be aware, and the knowledge you need to help protect cardholder data. You should learn to incorporate this knowledge into your daily activities. It will help you in your role here, as well as help to protect the information and resources which we are entrusted. The material presented here is important to each of us in our organization.

Securing Cardholder Data
PCI Data Security Standard: Objectives

After completing this course, you should be familiar with:

- An overview of PCI DSS,
- What is required of you as a Retail Jamboree Staff volunteer for the BSA,
- The potential issues facing the security of information,
- What steps are necessary to protect cardholder information,
- The fact that information security is part of your responsibility.

Securing Cardholder Data – What is PCI DSS?

PCI DSS, as established by the PCI Security Standards Council, is a set of association mandated requirements for the handling of credit card information and validation of merchant compliance. The PCI Security Standards Council is comprised of payment card brands such as Visa, MasterCard, American Express, Discover and JCB. This group maintains Data Security Standards (DSS) on transmitting, processing, and storing of credit card data.

As a merchant that accepts credit cards, the Boy Scouts of America must comply with the PCI DSS. Merchants are responsible for the security of cardholder data and must be careful not to store certain types of data on their systems or the systems of their third party service providers. Merchants are also responsible for any damages or liability that may occur as a result of a data security breach or other non-compliance with PCI DSS.

Securing Cardholder Data – Why Does PCI DSS Exist?

There are several reasons why PCI DSS was developed.

First, the payment card industry and merchants lose billions of dollars each year to fraudulent charges from stolen cards, card numbers and personal identity theft.

Second, the negative public exposure of a reported security breach can additionally cost an organization millions of dollars for ever one incident.

Third, for consumers, it will help reduce identity theft. If not prevented, it can cost an individual thousands of dollars and countless hours to correct. The most common type of identity theft is credit card fraud.

Securing Cardholder Data – What Can You Do?

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. There are six categories of PCI DSS compliance security standards. Each category has specific requirements which are listed on the following slide.

PCI DSS is important to the success of our organization.

- First, become familiar with PCI DSS and how to protect cardholder information.
- Second, incorporate these security practices into your everyday functions.
- Third, encourage co-workers to do the same.

Security is the responsibility of each person in our organization.

Securing Cardholder Data – Payment Card Industry Data Security Standards (PCI-DSS)

- **Build and Maintain a Secure Network.**

  Requirement 1: Install and maintain a firewall configuration to protect cardholder data

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

- **Protect Cardholder Data.**

  Requirement 3: Protect stored cardholder data

  Requirement 4: Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program.**

  Requirement 5: Use and regularly update anti-virus software

  Requirement 6: Develop and maintain secure systems and applications

Securing Cardholder Data – Cont’d
Payment Card Industry Data Security Standards (PCI-DSS)

- **Implement Strong Access Control Measures.**
  Requirement 7: Restrict access to cardholder data by business need-to-know
  Requirement 8: Assign a unique ID to each person with computer access
  Requirement 9: Restrict physical access to cardholder data

- **Regularly Monitor and Test Networks.**
  Requirement 10: Track and monitor all access to network resources and cardholder data
  Requirement 11: Regularly test security systems and processes

- **Maintain an InformationSecurity Policy.**
  Requirement 12: Maintain a policy that addresses information security

Securing Cardholder Data – Cardholder information Terminology

There are various pieces of information associated with each credit card and its owner. Retail Jamboree Staff volunteers should become familiar with these terms, as it will help in learning how to protect this information:

- Primary Account Number (PAN)
  This is the full 15-16 digit account number of the credit card. It identifies the issuer and the particular cardholder account
- Cardholder name
  This is the name of the individual (or entity) to whom the card was issued
- Service code
  This is a three or four digit number on the magnetic-stripe that specifies the acceptance requirements and limitations for magnetic-stripe read transactions
- Expiration date
  Is the date in which the card is no longer valid
- Full magnetic stripe
  The magnetic stripe or “magstripe” is on the back of payment cards, which stores data. The kind of data that the magnetic strip contains can be the cardholder’s name, account number, encrypted PIN, and other discretionary data
- CVC/CID
  This is the Card Validation Code on the signature panel located on the back of the card. It is calculated through a specific algorithm using information about the account
- PIN
  This is the Personal Identification Number associated with the card. It is a number usually selected by the cardholder, which acts as a password for certain devices (e.g., ATM, Debit card, etc.)

Securing Cardholder Data – Protect Stored Cardholder Data

The following table shows the elements of cardholder and sensitive authentication information. The table shows what elements can be stored subsequent to authentication and what safeguards must be taken.

	Data Element	Storage Permitted	Protection Required	Encryption Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	Yes *	No
	Service Code	Yes	Yes *	No
	Expiration Date	Yes	Yes *	No
Sensitive	Full Magnetic Stripe	No	n/a	n/a
Authentication	CVC2/CID	No	n/a	n/a
Data **	PIN/PIN Block	No	n/a	Na/

* These elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS required standards.

** Sensitive authentication data must not be stored subsequent to authentication (even if encrypted).

Securing Cardholder Data – Cardholder Information Storage

Data elements that can be stored include the Primary Account Number (PAN), the cardholder name, the service code and the expiration date. While these items are permitted to be stored, they must be protected at all times. The PAN must be rendered unreadable through the use of encryption, strong one-way hash algorithms, or truncation.

In addition, anytime the PAN is displayed or printed (point of sale receipt) the full number must not be shown and should be masked.

Example: **** **** **** 2936

Other Data elements that can be stored must also be stored in protected form if stored with the PAN.

Securing Cardholder Data – Data Retention and Disposal

Cardholder information storage should be for the minimum time necessary for the business function or for legal/regulatory compliance purposes. Destroy or mask any personal information that is not required. If using a credit card, once the credit card has been authorized, mask (or render unreadable) all of the numbers except the last four digits.

Sensitive authentication data must **NEVER** be stored after the transaction authorization process. These data items include the full magnetic stripe, the card validation code (CVC or CID), or the PIN or encrypted PIN block. Storage of these elements is strictly forbidden, even in encrypted form.

Securing Cardholder Data – Processing Credit Cards

Normally, we would advise you to never write down a customer’s credit card information. However, we understand that unique circumstances may arise and writing down a cardholder’s information is the only viable option. The following are acceptable circumstances for writing down a cardholder’s information:

- When a remote event is taking place and National Supply merchandise is sold, but a JDA POS register is not available.
- When the JDA POS system goes down because of a power outage, technical difficulties, etc.
- When a customer phones in an order.

Securing Cardholder Data – Processing Credit Cards

If one of those acceptable circumstances should arise, you must follow the process below to ensure that a customer’s credit card information is properly documented and kept secure:

- Capture the customers information by using a pink order form.
- Secure the completed pink order form in a safe location (e.g., locked filing cabinet).
- Process the customer’s credit card as soon as the JDA POS is available.
- Shred the customer's credit card information once the credit card has been processed.

Securing Cardholder Data – Processing Credit Cards

If you work in an area where you enter credit card orders via telephone or physically process credit card purchases, there are a number of things for you to keep in mind to protect the cardholder and their information.

By phone:

- Use a pink order form to properly document the customer’s order and credit card information.
- Secure the pink order form in a safe location.
- Enter the information directly into the processing system when available.
- Verify that an authorization code is returned before completing the transaction.
- Shred the customer’s credit card information once transaction is completed.

In person:

- Verify the identity of the cardholder.
- Do not write down any information from the card.
- Immediately return the card after the swipe transaction is complete.

Securing Cardholder Data – Restrict Access to Cardholder Data by Business Need-to Know

Cardholder information should only be accessible to those individuals who need it to perform their job.

Default access rights to cardholder data should be “Deny All” unless a user or group is specifically allowed. This access should be reviewed periodically for “need to know” applicability.

Securing Cardholder Data – Password Management

It is important to protect your password by following these guidelines:

- Do not share your password with anyone.
- Never write down your password.
- Change your password at least every 90 days.
- Do not re-use a password for at least four password change cycles.
- Do not store your password in a computer file.
- When receiving technical assistance, enter your password instead of telling it to the technical staff member.
- If you ever receive a telephone call from someone claiming to need your password, report it immediately.

Securing Cardholder Data – Managing User Authentication and Passwords

PCI provides stringent requirements for account and password management. These apply to all non-consumer users as well as administrator accounts.

PCI specifies that we:

- Properly manage and control the addition, deletion or modification of user IDs.
- Verify user identity before processing password reset requests.
- Utilize unique passwords during account/password creation or subsequent password changes.
- Immediately remove access for terminated users.
- Review and remove inactive accounts at least every 90 days.
- Require strong passwords.
- Minimum of 8 characters utilizing upper- and lower-case letters, numbers and special characters (if system permits)
- Users should be prohibited from re-using a password for four (4) password change cycles.
- Limit invalid login attempts to six then lock account for a minimum of 30 minutes.
- Disconnect login sessions that have been inactive for more than 15 minutes. Require password to re-activate connection.
- All cardholder database access must be authenticated, including users, administrators and applications.

Securing Cardholder Data – Audit Logs

Systems logs that document user access and activities are imperative in the event cardholder information is compromised. PCI DSS provides strict rules for the implementation of these logs.

For potential investigative purposes, an automated log audit facility should be implemented to identify:

- Individual user access to cardholder data.
- Any action by a user with root or admin access.
- Access to audit logs.
- Invalid access attempts.
- Use of ID and authentication.
- Initialization of audit logs.
- Creation and/or deletion of system-level objects.

Securing Cardholder Data – Deploy Anti-Virus Software on All Systems

With the dawn of e-mail, it quickly became the vehicle of choice for virus distribution. Now, virus authors are also creating malicious code that can be distributed through other means such as seemingly innocuous web sites, mini-applications such as games and even graphic pictures. Because of these vulnerabilities, it is important to maintain effective and up-to-date anti-virus software.

Every personal computer, server or any other machine that could be infected within our networks must have our standard anti-virus software installed before it is connected to our network.

Ensure that all anti-virus software is actively running, includes current updates and can produce an audit log, if necessary.

Securing Cardholder Data – Physical Access to and Security for Cardholder Data

Systems or printed reports that contain cardholder information must be physically secured at all times. Physical access must be controlled and provided based on job requirements. Uncontrolled access could provide the opportunity for unauthorized viewing, manipulating or even theft of this sensitive data.

PCI requires that video surveillance be utilized to monitor areas containing cardholder systems or work areas where this information may be handled or processed. The video media must be retained for at least three months unless otherwise restricted by law.

Never allow public access to wired network jacks or wireless access points for networks that connect to cardholder systems.

Securing Cardholder Data – Securing Computers and Media

Any form of device or media that contains cardholder information must be secured and tracked at all times. This includes:

- **Computers** – Computers should be physically secured to the work area, if possible. Each device should have an asset tag or ID tag. There should be an auditable log of to whom each device is assigned.
- **Mobile devices** – PDSs and other devices that could contain cardholder information should be reviewed for necessity in the workplace. If deemed necessary, these devices need to adhere to the access and encryption standards for PCI. A strict inventory and control system should be put in place prior to distribution or use. They should be physically secured at all times when not in use.
- **Portable media** – As with mobile devices, the use of portable media should be thoroughly reviewed for necessity before being implemented. If deemed necessary, these devices need to adhere to the access and encryption standards for PCI. A strict inventory and control system should be put in place prior to distribution or use. They should be physically secured at all times when not in use.
- **Paper files, reports or receipts** – Physically secure any paper-based media that contains cardholder information. Ensure that these items are also properly destroyed when discarded.

Securing Cardholder Data – Data Classification and Labeling

Securing Cardholder Data- Securing Computers and Media

The use of any modems or wireless technology to access any BSA system or processing resource which is within the cardholder data environment or contains any cardholder data, whether at third party hosting locations or BSA locations, requires the explicit written approval of the Senior IT Management of the BSA and Supply Group Help Desk.

Protection of Proprietary and Sensitive Data, Including Cardholder Data

Confidential information includes, but is not limited to: Information concerning the BSA employees and volunteers; cardholder data; and network configurations and specifications. Retail Jamboree Staff volunteers should take all necessary steps to prevent unauthorized access to this information.

When storage or displaying of cardholder data is requires, the Primary Account Number (PAN) must be encrypted or masked displaying either the first six and/or the last four numbers. Full track data shall never be stored or displayed on any device.

Securing Cardholder Data – Securing Computers and Media

Emailing card Holder Data

Never request or send unencrypted PANs (Primary Account Number) by end-user messaging technologies (e.g., email, instant messaging, chat, etc.). Ensure that strong cryptography is used whenever cardholder data is sent via end-user messaging technologies.

Enforcement

Retail Jamboree Staff volunteers are expected to conduct themselves according to the basic principles of the BSA as set forth in the Scout Oath and Law and to comply with specific regulations established for the benefit, protection and fair treatment of all employees and volunteers.

Rule violations may result in immediate suspension of employment and termination following verification of charges. Violations will result in formal disciplinary action, including documented warnings to file or discharge, depending on the nature and repetition of infractions.

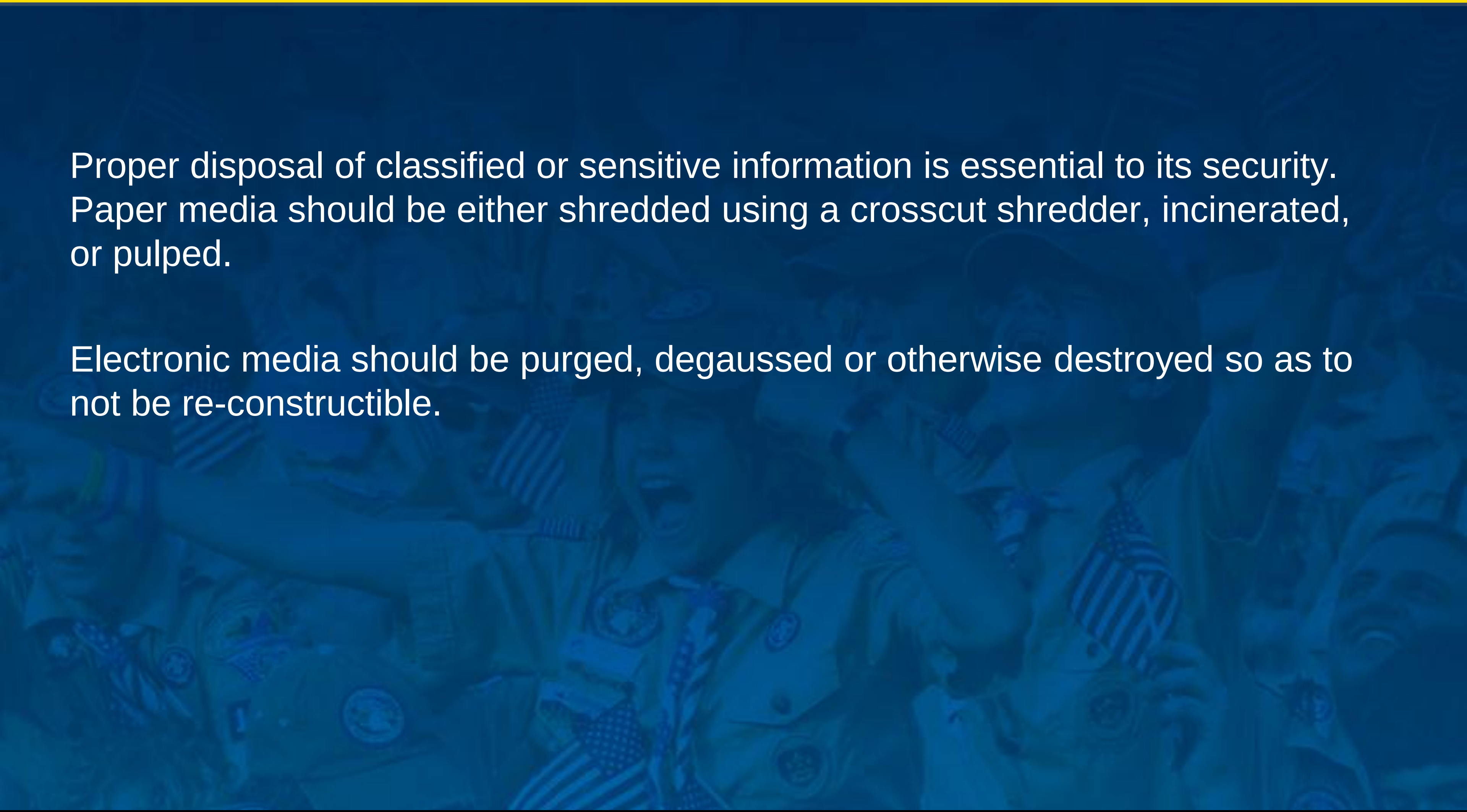
Securing Cardholder Data – Data Classification and Labeling

Data should be classified and labeled so it can be handled adequately. Any information that is considered sensitive should be given appropriate status and labeled as such. This classification would include any form cardholder information. Any media (electronic or paper) that contains classified information should be physically secured, logged and tracked.

Any classified media transport should be performed through a secured courier that can be accurately tracked.

Any storage or access to media with cardholder information should be strictly controlled and monitored.

Securing Cardholder Data – Data Destruction



Proper disposal of classified or sensitive information is essential to its security. Paper media should be either shredded using a crosscut shredder, incinerated, or pulped.

Electronic media should be purged, degaussed or otherwise destroyed so as to not be re-constructible.

Securing Cardholder Data – Visitors

It is important to be able to quickly identify and tell between employees and Retail Jamboree Staff volunteers and visitors. Access control badges are a good example of this type of system.

Be sure that visitor access is only granted after verified authorization. Access badges should be dated, logged and provided for a specified and expiring time period. The badges should be visible at all times and must be returned to the controlling authority, prior to leaving the physical premises.

All access should be logged for audit and investigation purposes, if necessary. These logs should be maintained for at least 3 months.

Securing Cardholder Data – Incident Reporting

Report if there is either a suspected or security breach of a BSA application or system in which payment card (credit card) or personal identifiable information has been compromised.

The following steps are to be taken in the vent of a system or security breach incident:

1.Any person who suspects or discovers an incident is required to immediately notify the BSA's Nation Service Desk as follows:

- If the reporting person is a member of the National Office, they should contact the National Service Desk at (877) 272-1910.

- If the reporting person is not a member of the National Office, they should contact the National Service Desk at (877) 272-1910.

Securing Cardholder Data – Incident Reporting

National Service Desk shall create an incident ticket and obtain following information:

- The name, location and contact information of caller.

- Date and time call was received.

- A brief description of the incident.

- What systems, applications, or equipment are involved.

Securing Cardholder Data – Information Security Policies

The backbone of security within any organization is the security policy. This document sets forth the rules by which our employees, contractors, vendors, and even Retail Jamboree Staff volunteers must conduct themselves when it comes to the security of our information resources.

PCI DSS requires that we create, maintain, publish and communicate a security policy that addresses the PCI DSS requirements, identifies threats and vulnerabilities, and is reviewed at least once a year.

Security policies should clearly identify responsibility areas for all employees, contractors, and Retail Jamboree Staff volunteers. A good security policy is clear, strong and supports the goals of the organization. It educates employees and Retail Jamboree Staff volunteers about the importance of information security and most importantly, their responsibility.