

MANAGING PAYMENT CARD AND POS SOFTWARE FOR PCI DSS COMPLIANCE

What Does This Mean to Me?

2/24/2010

TallySoft

Cindi Youngstead



MANAGING SOFTWARE AND PAYMENT ACCOUNT SECURITY

- Is your credit card software PCI compliant?
- Are you PCI compliant?
- Do you know what it takes to become compliant?
- Are you prepared to pay fines up to \$500,000?

WHO IS REQUIRED TO BE PCI COMPLIANT?

PCI DSS applies to **All** entities that store, process, and/or transmit cardholder data. As a merchant who accepts and processes payment cards, you must comply. The PCI DSS, *Payment Card Industry Data Security Standard*, was written by the "Payment Card Industry Security Standards Council," an organization formed to bring together requirements from all payment card brands into one standard. Compliance is required by:

- *Payment Card Brands*: AMEX, Discover, JCB, MasterCard, and Visa
- *Your Processor*
- *Your Acquiring Bank* (Merchant Services Provider)

Payment Cards include cardholder data for credit cards, debit cards, and prepaid cards.

WHO IS THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL AND WHAT DO THEY DO?

Founding members from each of the “Payment Brands” comprise the council:

- **American Express**
- **Discover Financial Services**
- **JCB International**
- **MasterCard World**
- **Visa Inc. International**

The PCI Security Standards Council (PCI SSC) is a global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security.¹

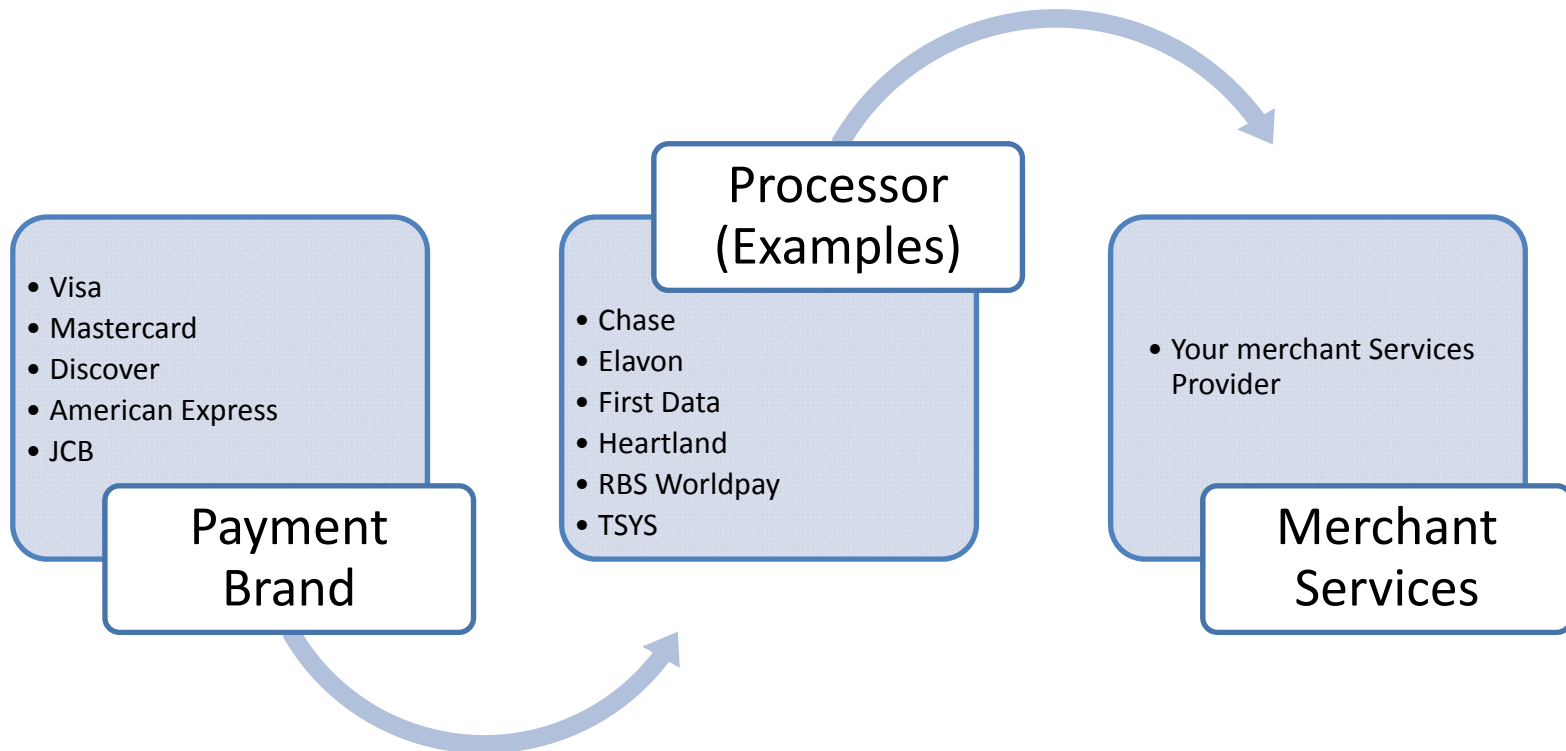
The Council maintains, evolves, and promotes the Payment Card Industry security standards.¹

The Council provides critical tools needed for implementation of the standards such as assessment and scanning guidelines, a self-assessment questionnaire, training and education, and product certification programs.¹

1. PCI Quick Reference Guide Understanding the Payment Card Industry, Data Security Standard version 1.2

DOES THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL ENFORCE COMPLIANCE?

No. Compliance is enforced at multiple levels, but not by the council. The chart below indicates the different entities involved in enforcing compliance.



WHAT HAPPENS IF I'M FOUND TO BE OUT OF COMPLIANCE?

That depends on how it is discovered...

- If you are found to be out of compliance during the discovery process, system scans, or audits, you are generally given the opportunity to resolve the issue without incurring any fines.
- Once you have been certified to be compliant, you are required to report a compromise. Failure to do so may result in a fine. Each *payment brand* determines if a fine is assessed and the amount of the fine.
- If you are found to be out of compliance due to a security breach, depending on the type and severity of the breach, you may be fined up to \$500,000 *per incident* plus the cost of forensic research. Again, each *payment brand* determines if a fine is assessed.

“Ensuring that you are compliant is the best way to combat fines and costs.”

HOW DO I BECOME COMPLIANT?

Compliance consists of twelve steps that must be maintained to ensure compliance.

Goals	PCI DSS Requirements
Build and Maintain a secure network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect shared cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software or programs 6. Develop and Maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for employees and contractors.

IS MY SOFTWARE PCI-DSS COMPLIANT?

Software companies must meet a different set of compliance standards; the *Payment Card Industry - Payment Application Security Standard*. These requirements complement the requirements that a merchant must meet. Below are examples of some of the requirements that Payment Applications must meet:

- Do not retain full magnetic strip, card validation code or value, (CAV2, CVV2, CID), or Pin Block data.
- Provide secure authentication features
- Protect wireless transmissions
- Facilitate secure remote software updates
- Encrypt sensitive traffic over public networks
- Maintain instructional documentation and training programs for customers

TALLYSALES

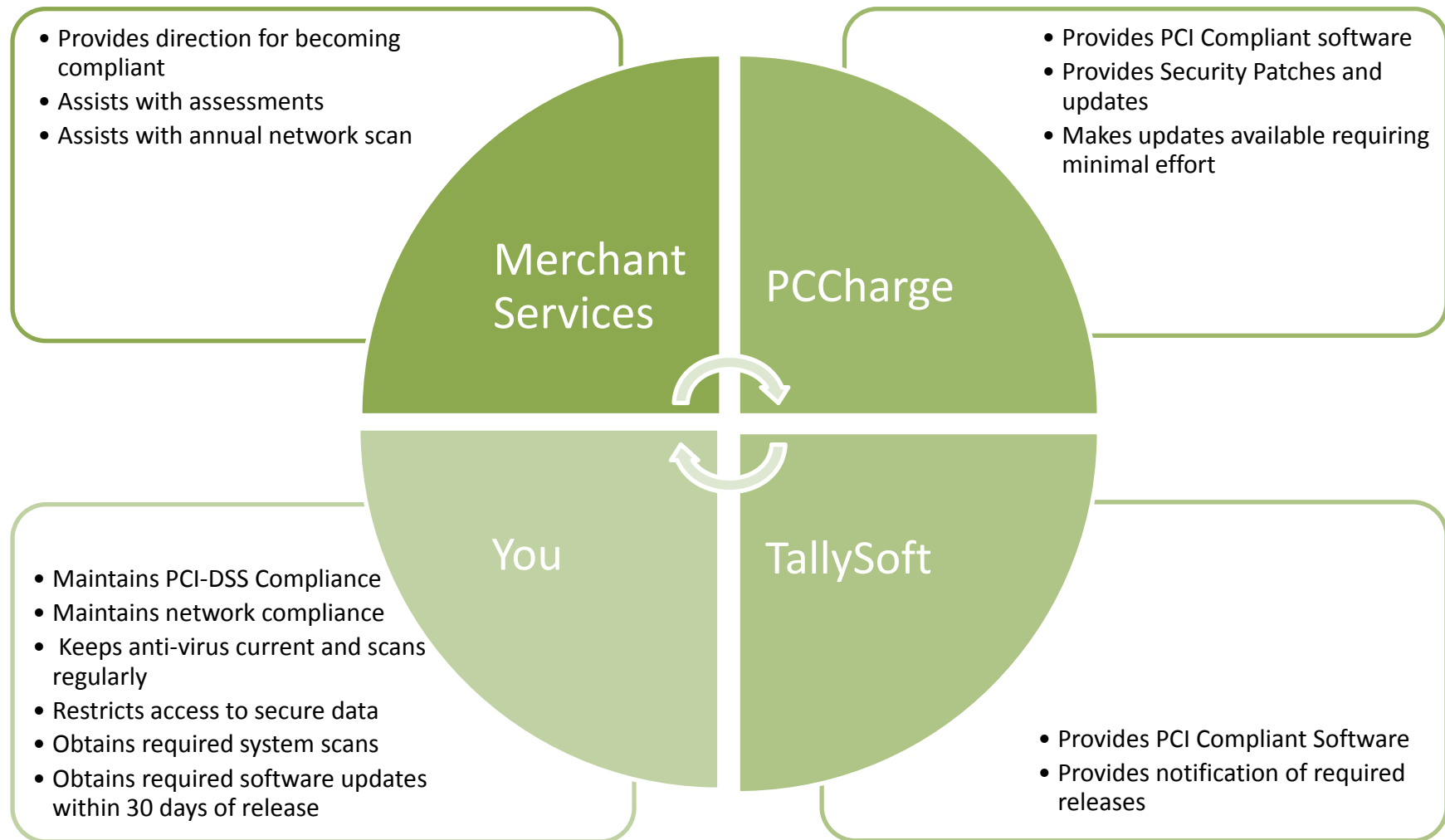
Current versions of TallySales, version 4.5.4 and above, meet PCI-PA SS requirements. Most importantly, both cardholder data and the PIN block, (debit cards), are encrypted. TallySoft provides access to cardholder information only when accessed by those with proper authority. Release information is forwarded to you via email when updates are released, including details of the updates made to the software. You will be notified in a separate email when security patches are released.

PCCHARGE PRO

PCCharge version 5.8x and higher is compliant with PCI-PA-DSS version 1.1. To meet the requirements for version 1.2, which must be met by July 1, 2010, you will need to upgrade to version 5.9. And unlike TallySales, which rarely needs to release Payment Card Security patches, PCCharge is constantly reacting to regulatory changes and security issues resulting in more frequent software updates. Included in the PCI requirements, you are required to update the software **within 30 days** of any new security patch.

WHO DOES WHAT?

Just as there are several levels of enforcement of PCI compliance, there are several levels of responsibility for ensuring compliance.



WHAT DOES ALL THIS MEAN TO ME?

Many years worth of research went into developing the compliance parameters put forth by the Payment Card Industry Security Standards Council. Security and technology issues arise continuously and the Council updates compliance requirements as the industry adjusts to address them. Having not gone through the required QSA, Tallysoft cannot interpret the information provided by the council; however we will assist you by providing information that will guide you in the process of becoming compliant, and provide support with regard to our software and PCCharge.

You are the key to becoming and maintaining compliance. The process is ongoing and requires constant attention. Small to mid-sized merchants are obligated to adhere to the same requirements as large merchants. Generally, that places the burden of maintaining compliance on fewer individuals, in addition to physical constraints that can make compliance almost impossible. As you go through the process of becoming compliant, ask your Acquiring Bank representative or consultant how to apply for modifications or exemptions from these requirements. Exemptions must be approved before compliance can be verified.

Please refer to the PCI Security Council's website at the following link to review compliance details:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

WHAT DO I DO NEXT?

In 2009, the amount of cardholder data that was compromised doubled that of 2007. A single breach can put a small company out of business. If you have not already begun, start the compliance process now. What needs to be done?

Note: *Links to all PCI DSS documents referenced in this section can be found in "Appendix A."*

1. Contact your Acquiring Bank to request information regarding PCI DSS Compliance and ask if they have any programs that will assist you with the process. Take advantage of all resources available to guide you with this task.
2. Determine your merchant "Level" based on the number of transactions performed annually.
 - a. **Level 1:** Greater than 6 million credit card transactions per year; any business that has suffered a hack or data breach; or any business deemed Level 1 by card associations.
 - b. **Level 2:** 1 to 6 Million credit card transactions per year.
 - c. **Level 3:** 20K to 1 Million credit card transactions per year.
 - d. **Level 4:** Less than 20K Ecommerce, or 1 Million total transactions per year.

WHAT DO I DO NEXT? Continued...

3. Complete the required assessment based on your merchant level:
 - a. For Level 1, a Qualified Security Assessor, (QSA), is required to facilitate and validate adherence to PCI DSS compliance. Annual assessments are required to maintain compliance. Your sales or merchant services representative may be able to recommend a QSA. You may also contact any QSA listed in the *Qualified Security Assessors* list found on the PCI Security Standards website.
 - b. For Levels 2, 3, and 4, complete the Self Assessment Questionnaire. For items where “no” is selected, prioritize and address each issue. Refer to the *Prioritized Approach...* documents provided by the Council to assist merchants with becoming compliant.
4. Contact a network specialist to review PCI-DSS documentation and update your network configuration to meet the requirements. Provide them with *The Prioritized Approach to Pursue PCI DSS Compliance* document for reference purposes.
5. Hire an Approved Scanning Vendor, (ASV), to perform the required scans and tests of your network. Contact your Acquiring Bank and ask the following:
 - a. Do they work with or recommend a specific ASV to perform the required scans?
 - b. Are there special rates for working with their partner ASV?
 - c. Can the cost of the scan be added to your monthly merchant account statement or will it be billed directly from the ASV?

WHAT DO I DO NEXT? Continued...

6. Purchase and/or update your Anti-Virus software on each computer in your network.
7. Fix and maintain any failed area of the scan. Your ASV will provide a report for your reference.
8. Contact Technical Support to ensure that your **TallySales** and **PCCharge Pro** software support is current.
9. Schedule necessary upgrades with your Technician.
10. Provide necessary reports to your Acquiring Bank.
11. **MONITOR SYSTEM ACTIVITY AND MAINTAIN THE SECURITY OF YOUR NETWORKS AND CARD INFORMATION!**

Keep in mind that you may be complaint today and a simple change to software or hardware can make you non-compliant. It is more important now than ever before to pay attention to your Merchant Account Statements/Notices and alerts from TallySoft or Verifone to stay informed about PCI DSS compliance.

GLOSSARY

Taken from: *Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms*

See *Appendix A* for location of complete document.

Acquirer: Bankcard association member that initiates and maintains relationships with merchants that accept payment cards

Anti-Virus Program: Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including viruses, worms, Trojan horses, spyware, and adware

Authorization: Granting of access or other rights to a user, program, or process

Cardholder data: Full magnetic stripe or the PAN plus any of the following:

- Cardholder name
- Expiration date
- Service Code

Compromise: Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected

Default password: Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known

GLOSSARY Continued...

Network Security Scan: Automated tool that remotely checks merchant or service provider systems for vulnerabilities. Non-intrusive test involves probing external-facing systems based on external-facing IP addresses and reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network

PAN: Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number

Password: A string of characters that serve as an authenticator of the user

Patch: Quick-repair job for piece of programming. During software product beta test or try-out period and after product formal release, problems are found. A patch is provided quickly to users

Penetration Test: Security-oriented probing of computer system or network to seek out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect identify vulnerabilities and suggest security improvements

PIN : Personal identification number

Policy: Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures

Vulnerability Scan: Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network

APPENDIX A – WEB RESOURCES

PCI-SSC Documents

PCI Data Security Standard (PCI DSS):

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Prioritized Approach for DSS 1.2 and Prioritized Approach Tool:

<https://www.pcisecuritystandards.org/education/prioritized.shtml>

Self Assessment Questionnaire:

<https://www.pcisecuritystandards.org/faq/index.shtml>

Qualified Security Assessors and Approved Scanning Vendors:

https://www.pcisecuritystandards.org/qa_asv/index.shtml

Supporting Documents:

- Glossary
- Navigating PCI DSS Document
- PCI DSS Summary of Changes
- PCI DSS 1.2 FAQs
- Attestations of Compliance/Validation – AOC – Merchants v1.2

https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml

APPENDIX A – WEB RESOURCES

Commonly Used Processors

Contact your merchant services department if your processor is not listed.

TSYS:

http://www.tsysacquiring.com/support_svcs/merchant_compliance_assistance.shtm

Heartland:

<http://www.heartlandpaymentsystems.com/pcicompliance>

RBS WorldPay:

<http://www.rbsworldpay.com/pcidss/>

Chase Paymentech:

http://www.chasepaymentech.com/portal/community/chase_paymentech/public/public_website/solutions/merchant_support_center_pages/payment_regulations_and_resources

Elavon:

<http://www.elavon.com/acquiring/unitedkingdom/merchant/pci-compliance.aspx>

First Data:

http://www.firstdata.com/en_us/about-first-data/media/announcements-/10-20-08

APPENDIX B – SAMPLE FINES

Visa Fines

Non-Compliance

- 1st violation: \$50,000.00
- 2nd violation: \$100,000.00
- 3rd violation: discretionary

Failure to report compromise: \$100,000.00

Egregious Violation: \$500,000.00

Storing Full Track Data

- \$50,000.00: initial fine
- \$100,000.00: monthly until issue is resolved

MasterCard Fines

Failure to comply with SDP mandate

- Level 1 merchants: up to \$25,000.00
- Level 2 merchants: up to \$5,000.00
- Level 3 merchants: up to \$5,000.00