Payment Card Industry Data Security Standard (PCI DSS)

Compliance Guide for Merchants

Presented by:

COMPLIANCE FORGE

www.ComplianceForge.com

Copyright © 2017. BlackHat Consultants, LLC

Table of Contents

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) OVERVIEW

WHAT IS THE PCI DSS?

The Payment Card Industry (PCI) Security Standards Council consists of the five major credit card brands:

- Visa
- MasterCard
- American Express
- Discover
- JCB International

The PCI Data Security Standard (PCI DSS) is an international standard established by the PCI to protect their clients' credit card data. The most fundamental concept of the PCI DSS is to ensure merchants build and maintain a secure network.

The PCI DSS affects every organization that accepts credit or debit cards. Regardless of your transaction volume, you must meet the basic PCI DSS compliance requirements, which include completing an annual self-assessment questionnaire, a quarterly network scan, and meet all the standards outlined by the PCI DSS.

WHY SHOULD I CARE ABOUT BEING COMPLIANT WITH THE PCI DSS?

The members of PCI Security Standards Council continually monitor cases of account data compromise. These compromises cover the full spectrum of organizations, from the very small to very large merchants and service providers.

A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations, including:

- Loss of the ability to process credit cards (e.g., revocation of Merchant account)
- Regulatory notification requirements
- Loss of reputation
- Loss of customers
- Potential financial liabilities (e.g., card replacement costs, fraudulent purchases, etc.)
- Litigation

WHAT DOES IT MEAN TO BE PCI DSS COMPLIANT?

For most Merchants, compliance with the PCI DSS is mostly through self-certification where the Merchant attests that his/her organization meets all the requirements to be considered compliant with the PCI DSS.

The Merchant should have evidence of due care and due diligence to support this self-certification:

- Due care examples include, but are not limited to:
  - Written information security policies
  - Accurate and current network diagrams
  - Developing an incident response plan
  - Installing antivirus on all systems
  - Limiting open ports on the firewall
- Due diligence examples include, but are not limited to:
  - Quarterly vulnerability assessments
  - Monthly software patching of systems
  - Annual Self-Assessment Questionnaire
  - Semi-annual firewall Access Control List (ACL) review

How Does The PCI Security Standards Council Control & Enforce The PCI DSS?

There are several components that go into allowing credit cards to function properly. The PCI Security Standards Council members make money off the parties involved by allowing them to participate in the network. By legal contract, each party agrees to abide by the rules set by the individual PCI Security Standards Council members.

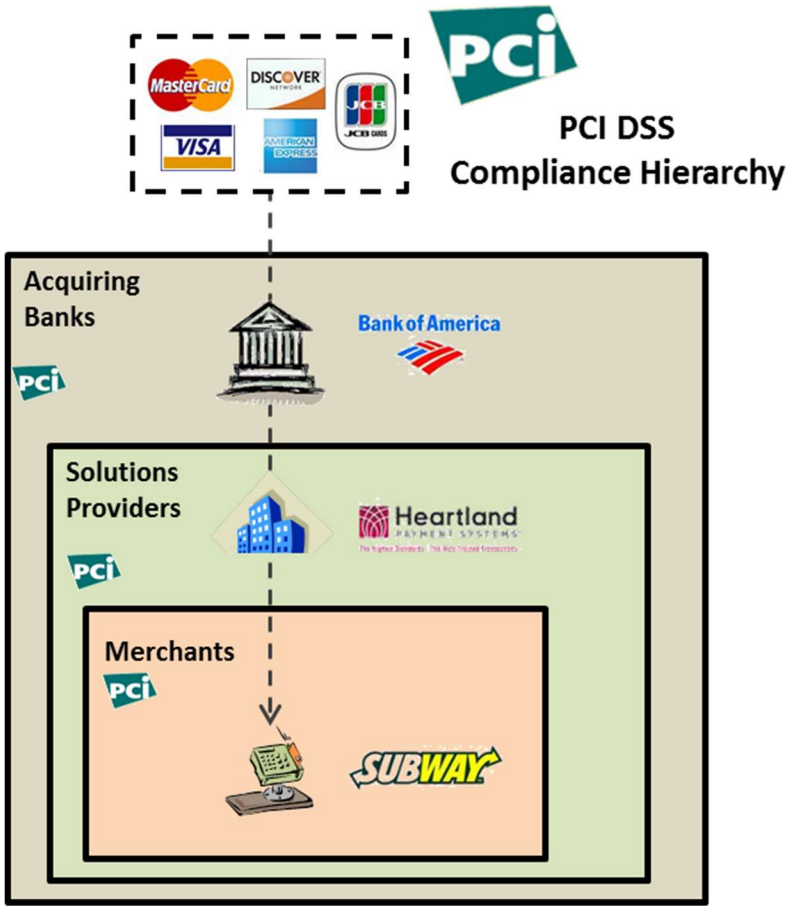
There is a Merchant side and there is a Consumer side to the process:

- Merchant Side
  - PCI member payment networks
  - Acquiring / sponsor banks
  - Solutions Providers
    - Credit card processors
    - Merchant Service Providers (MSPs)
    - Independent Sales Organizations (ISOs)
  - Merchants
- Consumer Side
  - Cardholder (consumer)
  - Issuing bank (who the consumer pays at the end of the month)
  - PCI member payment networks

PCI DSS Compliance Hierarchy

On the Merchant-side of the PCI DSS, all of the entities must be compliant with the PCI DSS since they do one or more of the following actions:

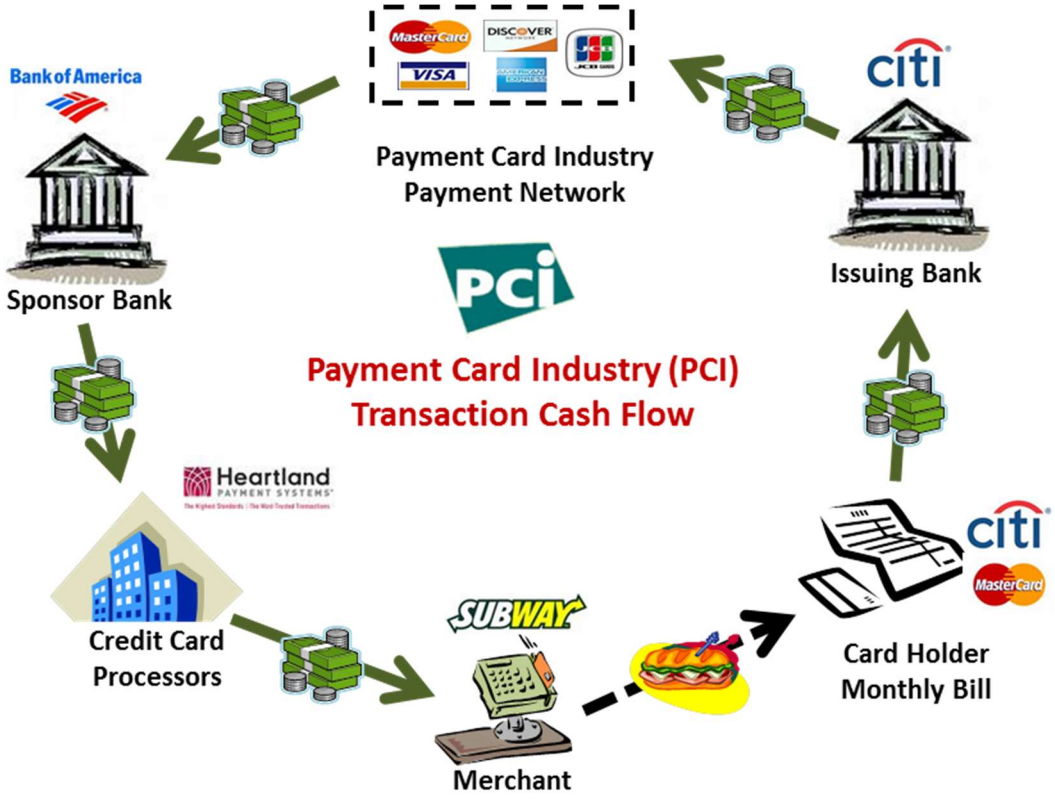
- Process payment card data
- Transmit payment card data
- Store payment card data



PCI TRANSACTION CASH FLOW EXAMPLE

In the following example, this shows that components necessary to buy something as simple as a sandwich with a credit or debit card:

1. The consumer uses a credit card to buy a sandwich.
2. The transaction is submitted to the credit card processor, which validates the credit card and limit.
3. The credit card processor pays the merchant within a few business days of the transaction.
4. The transaction goes through the sponsor bank, through the MasterCard payment network and eventually becomes a line item on the cardholder's monthly credit card statement, which the cardholder eventually pays.

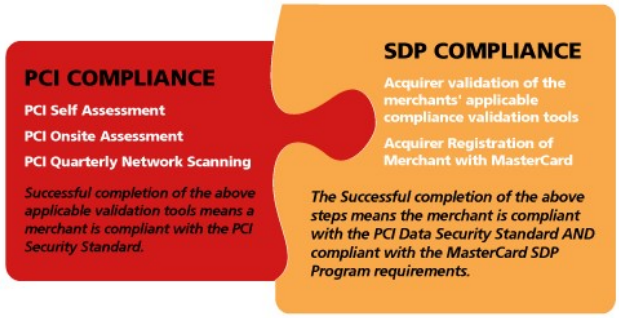


Note: If any party breaks the legal contract to be part of the network, the PCI Security Standards Council member has legal grounds to recoup losses or to banish an entity from being able to accept or process credit/debit cards.

This is the *real power* of the members of the PCI Security Standards Council – you have you comply with their rules or you are prohibited from being able to process transactions with their payment networks.

WHAT KIND OF MERCHANT AM I?

The "lowest common denominator" for minimum requirements is defined by MasterCard's Site Data Prevention (SDP) program. This sets the standard, since most Merchants accept both Visa and MasterCard at a minimum. Merchants must follow the most stringent requirements, which is the MasterCard SDP program.



The PCI Security Standards Council does not enforce the PCI DSS. Instead, the individual PCI Security Standards Council members are responsible for enforcing the PCI DSS through their own programs, such as MasterCard's SDP program or Visa's Cardholder Information Security Program (CISP).

The reason for this is MasterCard requires more complete PCI DSS compliance for Level 4 Merchants, as compared to other PCI members. If a Merchant accepts MasterCard, the Merchant must be both PCI DSS and SDP compliant.

Merchant Definition	Criteria	Onsite Review	Self Assessment	Network Security Scan
Level 1	- All merchants, including electronic commerce merchants, with more than 6 million total MasterCard transactions annually - All merchants that experienced an account compromise.	**Required Annually** [1]	Not Required	**Required Quarterly**[2]
Level 2	- All merchants with more than one million total MasterCard transactions but less than six million total transactions annually	Not required	**Required Annually**	**Required Quarterly**[2]
Level 3	- All merchants with annual MasterCard e-commerce transactions greater than 20,000 but less than one million total transactions	Not Required	**Required Annually**	**Required Quarterly**[2]
Level 4 [3]	**- All other merchants**	Not Required	**Required Annually**	**Required Quarterly** [2]

1. For Level 1 merchants, the annual onsite review may be conducted by either the Merchant's "internal auditor" or a Qualified Security Assessor (QSA).
2. To fulfill the network scanning requirement, all merchants must conduct scans on a quarterly basis using an Approved Scanning Vendor (ASV).
3. Level 4 Merchants are required to comply with the PCI DSS. Level 4 Merchants should consult their acquirer to determine if compliance validation is also required.

Note: Both the MasterCard SDP and the Visa CISP require all their merchants, including those in the Level 4 category, to be compliant with the PCI DSS. Both programs also require the annual Self-Assessment Questionnaire (SAQ) to provide documentation of compliance.

DOES THE PCI SECURITY STANDARDS COUNCIL REALLY CARE ABOUT SMALL MERCHANTS?

Yes! The PCI Security Standards Council setup a website especially for Small and Medium Businesses (SMBs) to help educated this demographic on their absolute requirements to protect cardholder data and the risks SMBs face for not being compliant with the PCI DSS: https://www.pcisecuritystandards.org/smb/

WHY IS COMPLYING WITH THE PCI DSS IMPORTANT TO MY BUSINESS?

PCI DSS compliance is a non-regulatory requirement. In layman's terms, a non-regulatory requirement is a legally-binding contract that you must uphold or you may be held in breach of contract.

Since non-compliance consequences can range from fines to devastating lawsuits, precautionary measures pale in comparison to the reactive costs associated with the aftermath associated with a PCI data breach when you are unable to demonstrate compliance.

If a Merchant is non-compliant at the time of an incident, the PCI Security Standard Council members (e.g. Visa or MasterCard) will hold the merchant liable for 100% of the fraudulent charges, as well as the costs to reissue credit cards to affected cardholders. Additionally, insurance will not cover the costs since the Merchant is negligent in fulfilling contractual requirements of the PCI DSS.

HOW CAN NON-COMPLIANCE VOID MY BUSINESS LIABILITY INSURANCE?

Insurance providers are in business to make money and will find ways to prevent paying out on claims. An easy way to avoid a costly payout for a breach is for an insurance company to demand proof of PCI DSS compliance at the time of the breach. Insurers know what it requires to be PCI DSS compliant and know what documentation and evidence is necessary to truly be compliant with the PCI DSS.

Most Merchants are unaware their insurance providers will not cover losses due to "negligent" behavior. This means the Merchant will be held entirely responsible for all losses, fines, and lawsuits, due to these negligence loopholes in their insurance coverage.

By failing to meet PCI DSS compliance standards that result in a data beach (e.g. identity theft), an attorney can easily demonstrate negligence on behalf of the Merchant. Negligence can be demonstrated by the Merchant's failure to meet the known standards. These objective benchmarks (e.g., PCI DSS requirements) set the standard for what constitutes negligent behavior in a court of law.

Note: Read your business liability insurance coverage for PCI DSS compliance. Your insurance provider may have additional requirements that you may have to address to ensure coverage is guaranteed.

WHAT HAPPENS IF I AM BREACHED, BUT I AM PCI DSS COMPLIANT?

Compliance with the PCI DSS serves as your "get out of jail free" card, where your insurance will cover your losses. PCI Security Standards Council members offer "safe harbor" protection from fines in the event a compliant Merchant experiences a data compromise.

To attain safe harbor status, Merchants must:

- Maintain full compliance at all times. This includes adhering to all requirements at the time of a breach or compromise, as demonstrated during a forensic investigation.
- Demonstrate that, before the compromise, the merchant or service provider already met the compliance validation requirements, demonstrating full compliance with the PCI DSS.

WHAT ARE EXAMPLES OF NON-COMPLIANCE AT THE TIME OF A BREACH?

Post-mortem compromise analysis has shown common security weaknesses that are addressed by the PCI DSS, but were not in place in the businesses and organizations when the compromises occurred. PCI DSS was designed exactly this reason—to minimize the chance of compromise and the effects if a compromise does occur.

These investigations consistently show common PCI DSS violations, including, but not limited to:

- Lack of Information Security standards. Formal standards were either not established or not enforced, which set the foundation for a misconfigured and improperly managed network (Requirement 12).
- Storage of magnetic stripe data (Requirement 3.2). It is important to note that many compromised entities are unaware that their systems are storing this data.
- Inadequate access controls due to improperly installed merchant POS systems, allowing hackers in via paths intended for POS vendors (Requirements 7.1, 7.2, 8.2 and 8.3).
- Default system settings and passwords not changed when system was set up (Requirement 2.1).
- Unnecessary and vulnerable services not removed or fixed when system was set up (Requirement 2.2.2).
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Requirement 6.5).
- Missing and outdated security patches (Requirement 6.1).
- Lack of logging (Requirement 10).
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems) (Requirements 10.6, 11.2, 11.4 and 11.5).
- Lack of segmentation in a network, making cardholder data easily accessible through weaknesses in other parts of the network (e.g., from wireless access points, employee e-mail, and web browsing) (Requirements 1.3 and 1.4).

How Do I Become PCI DSS Compliant?

What Are The Requirements Of The PCI DSS?

There are 12 sections of requirements that make up the PCI DSS:

1. Install & maintain a firewall connection to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software or programs
6. Develop & maintain secure systems and applications.
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.
10. Track & monitor all access to network resources & cardholder data.
11. Regularly test security systems & processes.
12. Maintain a policy that addresses Information Security for employees and contractors.

Note: each of these 12 requirements have multiple sub-requirements that must be met.

Are There Additional Steps To The PCI DSS That I Need To Know About?

Yes! In addition to the 12 sections, there are also several additional requirements. For smaller merchants, those additional requirements include:

- Performing a "quarterly" vulnerability assessment of your external IP addresses by an Authorized Scanning Vendor (ASV). *Note - See the section on vulnerability assessments for more details on this topic.*
- Conducting an annual Self-Assessment Questionnaire (SAQ) to self-certify your compliance with the PCI DSS

What Are The Real-World Steps to Becoming PCI DSS Compliant?

You need to meet ALL the requirements of the PCI DSS, perform the annual SAQ, AND perform a quarterly network scan. Only by meeting these three steps, will you be compliant with the PCI DSS.

Step 1: Implement a Written Information Security Program (WISP) or PCI DSS Security Policy to meet PCI DSS requirements 1 through 12
Step 2: Perform a quarterly, external vulnerability assessment by an Authorized Scanning Vendor (ASV)
Step 3: Complete the annual Self-Assessment Questionnaire (SAQ), based on Merchant type

What Is The Most Important PCI DSS Requirement?

Before you can become compliant with the PCI DSS, you need to have an overall information security program in place that protects your network from common vulnerabilities. This leads to Requirement #12 (Maintain a policy that addresses Information Security for employees and contractors) being the most important requirement, since those policies and procedures set the foundation for your company to be able to comply with the remaining 11 requirements.

The Written Information Security Program (WISP) or PCI DSS Security Policy from ComplianceForge.com addresses this requirement. The WISP serves as the foundation of an Information Security Management Program (ISMP) to address each of the requirements of the PCI DSS.

SELF-ASSESSMENT QUESTIONNAIRE (SAQ) OVERVIEW

WHAT ARE THE SAQ CATEGORIES?

According to payment brand rules, all merchants and their service providers are required to comply with the PCI DSS in its entirety. There are now **nine (9) different Self-Assessment Questionnaire (SAQ) categories**, shown in the table below, which help scope the attestation requirements as part of the annual SAQ validation.

SAQ Validation Type	Description	Total # of Requirements	ASV Vulnerability Scanning Required	Penetration Test Required
A	Card-not-present merchants: All payment processing functions fully outsourced. No electronic storage of cardholder data.	14	✗	✗
A-EP	** *NEW CATEGORY in v3.0*** E-commerce merchants re-directing to a third-party website for payment processing. No electronic storage of cardholder data.	139	✓	✓
B	Merchants with only imprint machines or only standalone dial-out payment terminals. No electronic storage of cardholder data or e-commerce solution.	41	✗	✗
B-IP	** *NEW CATEGORY in v3.0*** Merchants with standalone, IP-connected payment terminals. No e-commerce or electronic cardholder data storage.	83	✓	✗
C	Merchants with payment application systems connected to the Internet. No e-commerce or electronic cardholder data storage.	139	✓	✓
C-VT	Merchants with web-based virtual payment terminals. No e-commerce or electronic cardholder data storage.	73	✗	✗
D-MER	All other forms of receiving payment cards.	326	✓	✓
D-SP	** *NEW CATEGORY in v3.0*** SAQ-eligible service providers.	347	✓	✓
P2PE	Hardware payment terminals in a validated Point to Point Encryption (P2PE) solution only. No e-commerce or electronic cardholder data storage.	35	✗	✗

The PCI Security Standards Council provides an instructional guide on how to handle the SAQ process: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

What Is A Merchant Of Record?

A Merchant of Record (MOR) is a company that has a relationship with the payment processor. For most Merchants, they are the MOR, since the Merchant is the company that receives the proceeds from the customer when a credit card payment is settled.

The MOR is the company that is ultimately responsible for the financial transaction and is responsible for PCI DSS compliance.

What Are Examples Of SAQ Categories?

According to payment brand rules, all merchants and their service providers are required to comply with the PCI DSS. This applies to any form of method used to accept payment using credit or debit cards.

QuickBooks

For most default installations of QuickBooks, the Merchant would be required to perform a SAQ D and perform quarterly vulnerability scans against its external IP space.

QuickBooks Reference for PCI DSS:
http://support.quickbooks.intuit.com/OpenCms/sites/default/QBSupportSite/PDFs/PCI_PADSS_QB2010_Implementation_Guide.pdf

PayPal

Using PayPal still requires the Merchant to perform a SAQ A.

PayPal Reference for PCI DSS:
https://merchant.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=merchant/pci_compliant_solution

Custom Website

Having a customized, in-house website that accepts credit cards requires the Merchant to perform a SAQ D and perform quarterly vulnerability scans against its external IP space.

Quarterly Vulnerability Assessment Requirement Overview

What Is The Definition Of A Quarter?

According to guidance from the PCI Security Standards Council, one "quarter" is defined as 90 days and is not a calendar quarter.

> *PCI DSS Requirement 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).*

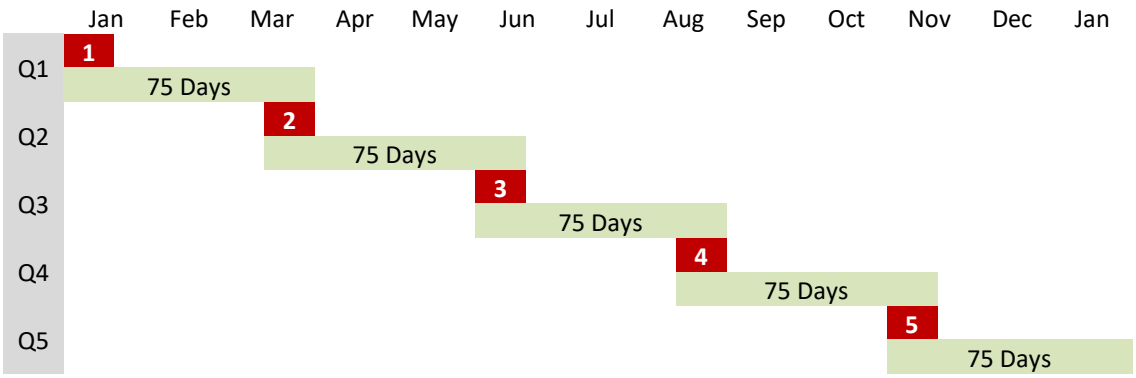
How Often Do I Really Need To Scan?

Since a PASSING scan is required every 90 days, it is recommended to add buffer time to allow for the remediation of any vulnerability that may have appeared since the last vulnerability scan.

With simple math, you will see that you need to perform at least five "quarterly" scans in a calendar year. Why is this? It is simple: 90 x 4 = 360 days of coverage.

It is recommended to perform a vulnerability scan no later than 75 days after the previous passing vulnerability scan, since that allows ample time to remediate identified vulnerabilities. This will help prevent the 90-day requirement from being missed.

The graphic below shows how five 75-day scan windows covers a complete calendar year, with ample room built in for addressing vulnerabilities:



Do I Really Need To Scan After A "Significant" Change?

Yes! If you install a new server, change firewall configurations or make other changes to the network that affects where your cardholder data is stored, transmitted or processed, you need to perform a PASSING external scan to demonstrate the change did not negatively affect your security posture.

What Is An Authorized Scanning Vendor (ASV)?

ASVs are companies who have tools that are certified to perform PCI DSS vulnerability assessments. Examples include:

- Comodo: http://www.hackerguardian.com (5 free quarterly scans)
- Trustwave: https://www.trustwave.com/pci-dss-merchants.php

Complete list of ASVs:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

IF I HAVE AN "ACCEPTABLE USE" POLICY ALREADY FOR MY EMPLOYEES, DOES THAT COVER THE PCI DSS REQUIREMENTS?

No! The PCI DSS is a very thorough set of requirements and an "acceptable use" policy might keep users from using workplace computers to surf pornographic websites, but is has no effect on other critical aspects of Information Security.

WHAT DOES A WRITTEN INFORMATION SECURITY PROGRAM (WISP) DO?

A Written Information Security Program (WISP) is one key ingredient to proving due care and due diligence on behalf of a Merchant.

Certain industries must meet strict regulatory compliance requirements (e.g. HIPAA, GLBA, SOX, SEC & FACTA). Regardless if a business is in a regulated industry or not, if that business accepts credit or debit cards then that business requires a professionally written set of policies, procedures, standards, and guideline. This is a non-negotiable requirement of the PCI DSS.

The PCI DSS actually has unique requirements which are more restrictive than other common regulatory requirements. For example, a chiropractor that maintains HIPAA compliance or a CPA that maintains GLBA compliance would have to adopt additional Information Security precautions to meet PCI DSS requirement minimums.

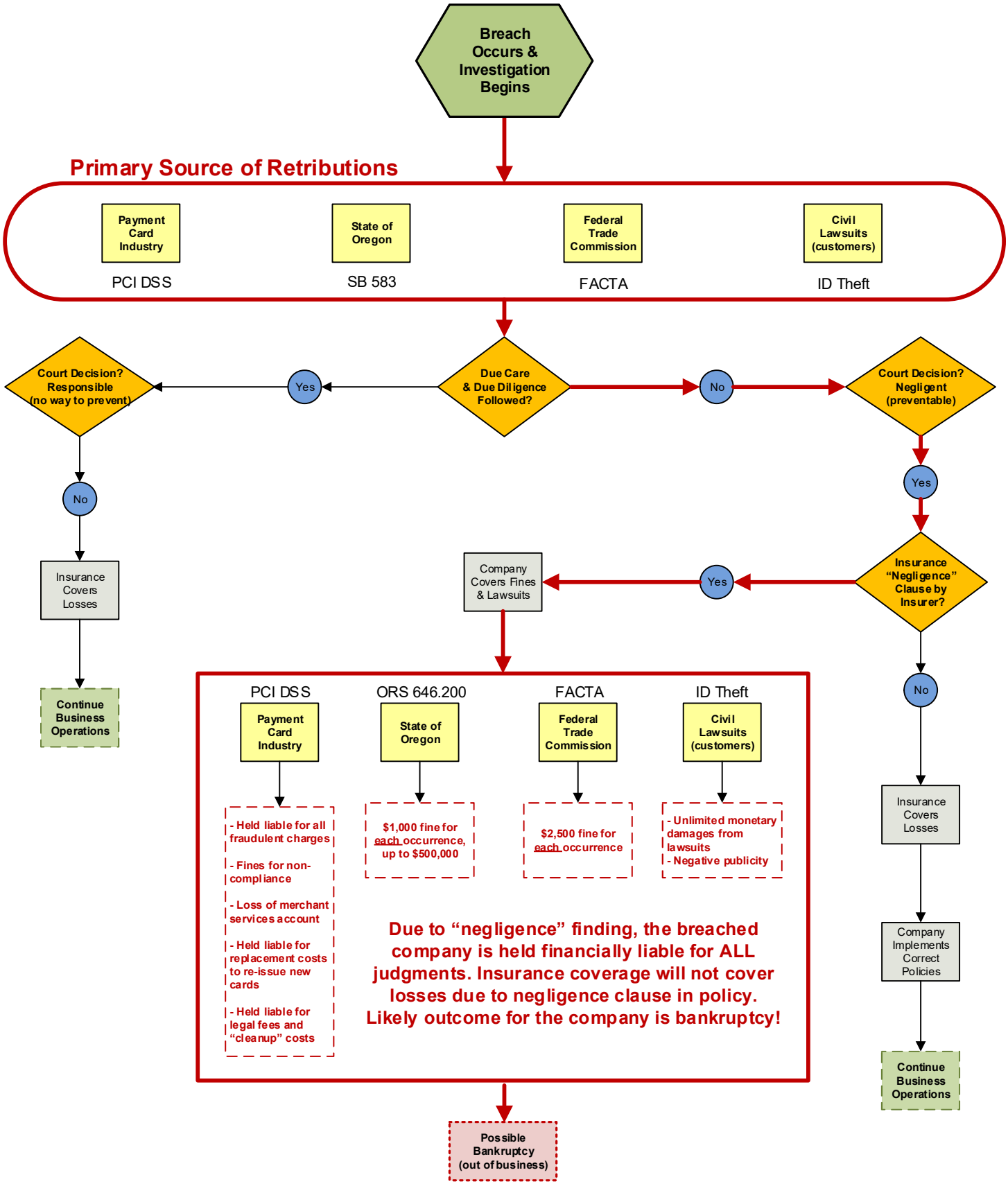
Documentation and training are proven to reduce the liabilities associated with Information Technology (IT) security threats. Purchasing and implementing a Written Information Security Program (WISP) demonstrates due care and due diligence on behalf of a Merchant.

This is crucial to reduce liability from a data breach or even employee misdeed:

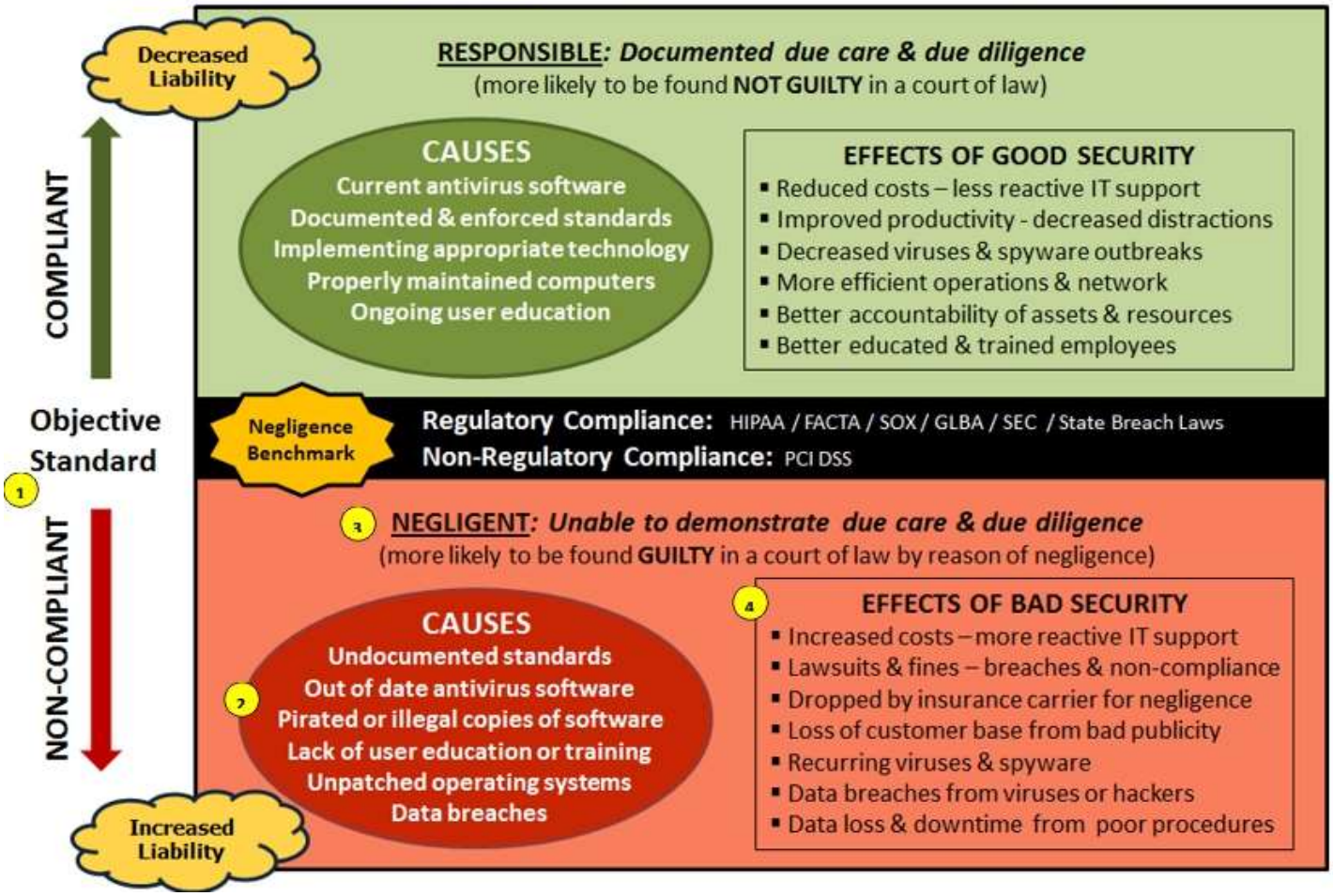
Preventative steps: Due care is the care and forethought a reasonable individual would exercise under the circumstances. It is the standard for determining legal duty. Demonstrating a proactive approach to mitigate risk by implementing policies, procedures, standards, and guidelines proves due care on behalf of the Merchant.

Ongoing steps: Due diligence is the effort made by a reasonable individual to avoid harm to another party, where failure to make this effort may be considered negligence. Implementing and enforcing policies, procedures, standards, and guidelines demonstrates due diligence by the Merchant.

DATA BREACH FLOWCHART: BREACH INVESTIGATION & RAMIFICATIONS



The goal of an Information Security program is to *decrease liabilities* while at the same time *improve operational efficiency*. This equates to bottom line savings for organizations!



1 If your company accepts credit cards, advises on financial matters, provides healthcare services, or maintains any Personally Identifiable Information (PII) on clients, then you are responsible for certain compliance requirements. These standards that are set by the regulation or requirement establish the foundation for a benchmark that will be used as an objective standard.

2 If your company does not meet the standards of the benchmark, that compliance failure is evidence of professional negligence. Negligence can be as simple as outdated antivirus software, weak passwords, weak wireless encryption standards, unpatched operating systems, or no Information Security policies. Each regulatory and non-regulatory requirement has its own unique standards.

3 Negligence is demonstrated by a lack of due care and due diligence on your company's part. A prosecuting (plaintiff) attorney's aim is to prove negligence. Without documented due care and due diligence, the task is made easier for the prosecutor to win a verdict of negligence for the plaintiff. The ability to prove negligence will allow damages to be awarded to the plaintiff.

4 The ramifications of a "negligence" ruling are devastating for a company, since most insurers have a "negligence clause" built into insurance policies. This precludes insurers from having to pay out for damages incurred due to the negligence of their policy holders. In simple terms, this means the company must pay all fines, damages, and legal fees on their own, without any insurance reimbursement.

How ComplianceForge.com Can Help You Become Compliant

Who Is Compliance Forge?

ComplianceForge.com is a website dedicated to Information Security for small and medium businesses.

We have a focus on the Payment Card Industry Data Security Standard (PCI DSS), since Requirement #12 of the PCI DSS requires all Merchants to "maintain a policy that addresses Information Security for employees and contractors."

We provide a Written Information Security Program (WISP) or a PCI DSS Security Policy that any business or organization can implement to meet this mandatory Merchant requirement.

Our goal is to be a source for Merchants to affordably obtain a comprehensive set of information security policies, standards, procedures, and guidelines that will allow the Merchant to meet requirements for the PCI DSS and other regulatory requirements.

You can buy a Written Information Security Program (WISP) or PCI DSS Security Policy from ComplianceForge.com to meet requirements 1 through 12 of PCI DSS version 3.

Documentation Is The Foundation of a PCI DSS Compliance Program

Before you can become compliant with the PCI DSS, you need to have an overall information security program in place that protects your network from common vulnerabilities.

In version 3 of the PCI DSS, there are multiple requirements (at least one in each of the 12 sections) that calls out the need for policies, standards and procedures. Those information security policies, standards and procedures set the foundation for your company to be able to comply with the remaining requirements.

The Written Information Security Program (WISP) or PCI DSS Security Policy from ComplianceForge.com addresses this requirement. The WISP serves as the foundation of an Information Security Management Program (ISMP) to address each of the requirements of the PCI DSS.