## Case Study:

# Lab – Case Study on PCI DSS Noncompliance: CardSystems Solutions

## Introduction

Payment Card Industry Data Security Standard (PCI DSS) is a compliance standard that helps prevent private data breaches in companies. Before PCI DSS was drafted, each credit card company had its own security requirements. Any merchant wanting to accept that company's credit card would need to comply with the company's security requirements. Merchants wanting to accept multiple credit cards grew frustrated by having to comply with multiple sets of requirements. To assist merchants, card companies sought a solution.

The solution began with the major credit card companies collaborating to form a representative group, now called the PCI Security Standards Council. Commonly called the PCI Council, they drafted and approved the standard, the PCI DSS. It's important to remember that the PCI Council is a group of companies, not a government agency. While the PCI Council is a group, only the individual credit card company can enforce PCI DSS on its own card. Instances of noncompliance are dealt with through penalties.

> CardSystems Solutions, a third-party payment processor, collected thousands of transactions of small and medium businesses. These transactions were then processed as batches and sent to credit card providers (such as Visa and MasterCard). The company's collection and processing of private information and financial data made it a prime target of potential hackers. Because of this, the company had to meet the data security standards that the federal, state, and industry standards require. Compliance is not optional for companies such as CardSystems Solutions.
>
> In June 2004, an external auditor certified the company as Payment Card Industry Data Security Standard- (PCI DSS-) compliant. The PCI DSS standards include installing a firewall and antivirus software and updating virus definitions on a consistent schedule. Companies must also encrypt privacy data elements. The company's certification implied that it followed a high standard of security, meaning the company used encryption methods to store privacy data. However, after the breach, a security assessment was

conducted. This assessment of the security measures used at the company proved that the company was not PCI DSS-compliant.

The hacker who performed the attack used a basic exploit known as a Structured Query Language (SQL) injection, which allows the hacker to place a snippet of code into the application. The hacker gained access through a Web application that customers used to access their data. With the code inserted into the fields of a form, the hacker was able to send SQL commands to the backend SQL server. The hacker wrote a script that gathered credit card data from the database, put it in a compressed ZIP file, and sent the credit card data to the hacker community through a File Transfer Protocol (FTP) site. The impact of the attack almost caused the company to go out of business. It had to eventually be acquired by another business.

These types of SQL injection attacks can be mitigated. Quality Web site design, secure coding, and internal firewalls all contribute to mitigating these types of attacks. The PCI DSS standard requires these types of mitigation controls and security methods. CardSystems was supposedly in compliance with the PCI DSS standard; however, if the company were in compliance, a successful SQL injection attack would mean the firewall was somehow circumvented.

CardSystems stored unencrypted data and failed to use proper security firewalls. It also failed to maintain its antivirus definitions. As a result, the FTC found CardSystems Solutions and its predecessors negligent and in violation of the FTC Act 15, U.S.C. §§ 41-58.

**Federal Trade Commission Act** (15 U.S.C. §§ 41-58, as amended)

Under this act, the commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress.

In this lab you will conduct a review of the literature on this topic and complete a literature review on this topic. There are many sites that can assist in the formatting and content of a literature review. Here is an example: http://guides.lib.ua.edu/c.php?g=39963&p=253698

Some of the questions to consider are:

1. What is the business problem/issue formulated by the author?

2. Is it clearly defined?

3. Could the problem have been approached more effectively or from another perspective?
4. Has the author also evaluated the literature relevant to this problem/issue?
5. Does the author agree or disagree with the relevant literature?
6. How does the article contribute to your understanding of the problem or topic?

Make sure to provide a reference slide that provides APA citations of any sources used in the PowerPoint presentation. This slide does not require narration.

**Literature Review Expectations:**

1. At least 10 peer-reviewed articles are to be included in the literature review.
2. It should be organized by theme or subject of the article.
3. A minimum of one paragraph is required per article is required.
4. The review must be synthesized, and the articles analyzed for content as it relates to the content of the case study above.
5. Free of grammatical errors.
6. **No evidence of plagiarism.**
7. Since this is Information Technology related the articles cannot be greater than 5-years old unless it considered a seminal article.
8. The literature review must be run through the plagiarism detector and no more than 25% of the articles should be used by another student. If there is a greater than 25% match in the paper it will receive a point deduction of 50%. If greater than 50% is a match the submission will receive a 0 without an option for resubmission. If there is a match in articles the synthetization and analyzation of the material MUST be original for content.

**Written Requirements**

Be sure to use appropriate APA format and cite your Reading or other sources that you used in your literature review.

The literature review should contain enough information to adequately answer the business problem provided in the case study and contain no spelling, grammar, or APA errors.  Points deducted from grade for each writing, spelling, or grammar error are at your instructor's discretion.

**Also review the university policy on plagiarism. If you have any questions, please contact your professor.**

**Directions for Submitting Your Lab**

Place your literature review in the drobox for the Unit 3 Lab.