IGI PUBLISHING **ITJ 5172**

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 3, Issue 2
edited by **Hamid Nemati © 2009, IGI Global**

PCI Compliance:
Overcoming the Challenges

Benjamin Ngugi, Suffolk University, USA

Gina Vega, Salem State College, USA

Glenn Dardick, Longwood University, USA

ABSTRACT

This study reviews the progress made by the introduction of the Payment Card Industry (PCI) compliance rules in the USA. Available data indicate that compliance has grown but several issues remain unresolved. These are identified within, along with an analysis of the feasibility of several solutions to the challenges that have hampered compliance with the Payment Card Industry rules. These solutions are evaluated by the extent to which they can help the merchants meet their business objectives while still safeguarding the credit card data. The first solution involves upgrading the current PCI standards as suggested by the PCI council. The second solution would require moving the burden of credit card information storage to the credit card companies and member banks, as suggested by the National Retail Federation. A third option reflects a socially responsible approach that protects the interests of all stakeholders. The study concludes by suggesting the way forward. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Authorization, Computer Crime, Data Protection, Data Security, Date Encryption, Electronic Commerce privacy , Hacker, Internet privacy, Privacy Laws, Privacy Regulations, Privacy Rights, Security Management, Security Risk*

INTRODUCTION

The credit card companies are struggling to fight data breaches, yet statistics for the last four years show that the number of data breaches continue to rise (Identity Theft Resource Center, 2005, , 2006, , 2007, , 2008). Specifically, these reports show that there were 158 cases of reported data-breaches in 2005, which rose to 315 and then to 446 cases in 2006 and 2007 respectively. As of August 2008, 449 data breaches were reported suggesting that the situation is continues to worsen.

The loss of credit card information is the focus of this study. Not all data breaches result in such a loss; however, just a single breach can result in the loss of millions of credit card records. A recent such example was the TJX Companies, Inc. computer intrusion during which more than 45 million customer records were affected (Privacy Commissioner -Canada & Information & Privacy Commissioner-Alberta, 2007). As of

August, 2007, the company had already spent about $256 million installing the necessary security systems to deter another attack and in meeting other costs associated with the intrusion, such as legal settlements and fines (TJX Incorporation, 2007). The figure is expected to increase, with some suggesting that the final cost may reach $1 billion (Goodin, 2007). Clearly, we are dealing with real threats that have dire financial consequences, and there is need for concerted effort from all stakeholders. This study contributes to this effort by identifying specific challenges hampering the security efforts by the card companies and suggests possible solutions to these challenges.

HOW DOES THE CREDIT CARD INDUSTRY OPERATE?

There are several major players in the credit card industry chain (Shift4 Incorporation, 2008). At the center of the chain is the customer who gets a credit card from the *issuer* (the financial institution that issues the credit card to the customer). The customer presents the credit card to the *merchant* in order to purchase a service or product. The merchant transmits this information to the *merchant bank* (also called the *acquirer*) for subsequent transmission to the *issuer,* who either approves or declines the request. This decision is transmitted back the same chain to the customer. The acquirer charges the merchants a fee in the form of a discount rate for acting as the middleman and then gives the issuer and the card companies a designated percentage of this fee. A significant aspect of the work of credit card companies such as VISA is to design regulations for the use and acceptance of credit cards.

Customers shopping at brick and mortar stores have to swipe their credit cards at the point of sale (POS) system when purchasing goods. This captures the full magnetic track data on the credit card (cardholder name, credit card number or primacy account number (PAN), expiration date, and other optional data). This is the most precious data for data thieves because it enables them to make counterfeit cards which can be used just like the real ones. On the other hand, e-commerce customers shopping on the Internet have to enter their names, credit card numbers, expiration dates and their security codes which are transmitted over the web to the acquirer (merchant bank) via the merchant. This is the second most important set of data for the card data thieves because it enables them to make fraudulent online purchases undetected.

Merchants may want to store the credit card data for several reasons. The primary reason is to meet the requirement by the credit card companies for the merchants to store credit card information data for up to 18 months in the event that there are disputes with the customers or other retrieval requests (Hogan, 2007). Secondary reasons include the desire of online retailers to offer quick check-out and automatic bill payment options to returning customers. These options would not be possible without storing the customer credit card information during enrollment and retrieving it on demand. The reality is that the stored information accumulates over time and becomes a magnet for criminals.

Credit card companies have to protect these data, both to prevent the criminals from using them to make counterfeit cards and also to retain the integrity of the credit card system. The credit card companies initially established individual proprietary programs for the storage of this data. This meant that merchants had a different set of rules from every credit card company, resulting in confusion for the merchants who had to implement different procedures from each credit card company. The rising confusion and increasing number of data breaches prompted the five major credit card companies to form a common body to pursue their common interests in reducing card fraud (PCI Compliance Guide, 2008). The five companies (VISA, MasterCard, American Express, Discover Card and JCB International) came together and formed the PCI Council in 2004. The council created the first payment standard called Payment Card Industry Data Security Standard (PCIDSS) two years later. These regulations apply to every