WHITE PAPER

PCI DSS made easy

Addressing the Payment Card Industry Data Security Standard (PCI DSS)

Major credit card companies are pushing hard to stop the financial fraud incidents that have affected numerous organizations and their consumers. Consequently, organizations that accept payment card transactions are duly bound to comply to PCI DSS by end of 2007. Organizations that fail to comply, risk not being allowed to handle cardholder data and fines of up to $500,000 if the data is lost or stolen. This white paper examines the necessary requirements to adhere to PCI DSS, the implications of non-compliance as well as how effective event log management and network vulnerability management play a key role in achieving compliance.

Introduction

Credit cards are widespread and their use for online payments is increasing dramatically. There were 1.3 billion credit cards in circulation in the U.S. in 2004, with 76% of Americans having at least one credit card. Retail U.S. e-commerce sales in the fourth quarter of 2006 were $33.9billion, a 25% increase over the same quarter in 2005.

There is bad news however: Credit card fraud (25%) was the most common form of reported identity theft in 2006. Considering that more than $48 billion was lost by financial institutions and businesses in that year due to identity theft, and $5 billion lost by individuals, it can be said that credit card fraud is digging deep into everyone's pockets! E-commerce fraud is also on the rise, reaching $3 billion in 2006 with an increment of 7% over 2005. This white paper examines the consequences of cardholder data theft and addresses the following key questions:

- What is the PCI directive?
- Why is it important for your business to comply?
- What are the consequences of not complying?
- What solutions are available to address the PCI directive?

Cardholder data theft and fraud – some real cases

- February 18, 2005 – Bank of America claimed that it had lost more than 1.2 million customer records – though it said there was no evidence that the data had fallen into the hands of criminals.

- June 16, 2005 – CardSystems, a merchant payment-processing provider, was sued in a series of class action cases alleging that it failed to adequately protect the personal information of 40 million customers. CardSystems' business faced collapse as VISA and American Express cut their ties with the company, prohibiting it from processing their card data. CardSystems was subsequently acquired by another company.

- February 9, 2006 – It was estimated that around 200,000 debit card accounts were disclosed by unknown retail merchants, apparently OfficeMax and others. These included accounts related to bank and credit union acquirers nationwide such as CitiBank and Wells Fargo.

- January 31, 2006 – Boston Globe and The Worcester Telegram & Gazette unwittingly exposed 240,000 credit and debit card records along with routing information for personal checks printed on recycled paper used in wrapping newspaper bundles for distribution.

- January 12, 2007 – MoneyGram, a payment service provider, reported that a company server was unlawfully accessed over the Internet last month. It contained information on

about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers.

- January 17, 2007 – TJX Companies Inc. publicly disclosed that they had experienced an unauthorized intrusion into the electronic credit/debit card processing system. In what is considered the most glamorous security breaches to date, as much as 45,700,000 credit/debit card account numbers and over 455,000 merchandise return records (containing customer names and driver's license numbers) were stolen from the company's IT system.

Large online retailers are not the only organizations being targeted. Public attention may be fixed on high-profile data losses, but experts studying financial fraud say hackers increasingly are targeting small, commercial websites. In some cases, criminals are able to gain real-time access to the websites' transaction information, allowing them to steal valid credit card numbers and quickly effect large numbers of fraudulent purchases. Small e-businesses offer fewer total victims, but they often present a softer target, either due to flaws in the software merchants use to process online orders or an over-reliance on outsourced website security.

Cybercrime and the attendant threat of identity theft reduce user and consumer confidence, slowing the acceptance of e-commerce. As a result, computer security, a critical activity that helps to protect these systems, has rightfully moved to a position of prominence.

Payment Card Industry (PCI) directive

The Payment Card Industry (PCI) data security framework was created by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. Prior to 2004, each of the associations had a proprietary set of information security requirements which were often burdensome and repetitive for participants in multiple brand networks. The associations subsequently created a uniform set of information security requirements for all national card brands (exclusive of boutique and private labels). These requirements became known as the PCI Data Security Standard (PCI DSS), governing all the payment channels: Retail, mail orders, telephone orders and e-commerce.

The PCI DSS framework

The PCI DSS framework is divided into 12 security requirements (VISA refers to them as the 'Digital Dozen') which are organized in six categories as follows:

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 or programs
Requirement 6: Develop and maintain secure systems and applications
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 information security policy
Requirement 12: Maintain a policy that addresses information security for employees and contractors

Table 1: The PCI DSS framework

Compliance with these requirements can be summarized into 3 main stages:

- **Collecting and storing**: Secure collection and tamper-proof storage of all log data so that it is available for analysis.

- **Reporting:** Being able to prove compliance on the spot if audited and present evidence that controls are in place for protecting data.

- **Monitoring and alerting:** Have systems in place such as auto-alerting, to help administrators constantly monitor access and usage of data. Administrators are warned of problems immediately and can rapidly address them. These systems should also extend to the log data itself – there must be proof that log data is being collected and stored.

Merchant and service provider levels

Merchants and service providers who must comply with the PCI DSS are categorized according to the number of card transactions they process over a 12-month period. Table 2 and Table 3

below describe the various levels and compliance requirements for both merchants and service providers.

Merchants are authorized acceptors of cards for the payment of goods and services. Examples of industries in which merchants must be compliant include, but are not limited to:

- Online trading such as Amazon.com online retailer
- Retail such as Wal-Mart retail outlets
- Higher education such as universities
- Healthcare such as hospitals
- Travel and entertainment such as hotels and restaurants
- Energy such as gas stations
- Finance such as banks and insurance companies

MERCHANT LEVELS	
MERCHANT DEFINITION *	COMPLIANCE
Level 1	
• Merchants from whom cardholder data has been compromised • Merchants with more than six million credit card transactions annually across all channels, including e-commerce	Annual onsite PCI data security assessment and quarterly network scans
Level 2	
• Merchants with between 1 and 6 million credit card transactions annually	Annual self-assessment and quarterly network scans
Level 3	
• Merchants with between 20,000 and 1,000,000 credit card e-commerce transactions annually	Annual self-Assessment and quarterly network scans
Level 4 **	
• All other merchants	Annual self-assessment and annual network scans

Table 2: Merchant levels

* Merchant levels are based on Visa USA definitions

** The PCI DSS requires that all merchants perform external network scanning to achieve compliance. Acquirers may require submission of scan reports and/or questionnaires by level 4 merchants.

Service Providers are organizations that process, store, or transmit cardholder data on behalf of card members, merchants, or other service providers. Examples of service providers which must be compliant include, but are not limited to:

- Payment gateways
- E-commerce host providers
- Managed service providers
- Credit reporting agencies
- Backup management companies
- Paper shred companies

SERVICE PROVIDER DEFINITION	COMPLIANCE
Level 1	
All processors (member and non-member) and all payment gateways.*	Annual onsite PCI Data Security assessment and quarterly network scans
Level 2	
Any service provider that is not in Level 1 and stores, processes, or transmits more than 1 million credit card accounts/transactions annually	Annual onsite PCI Data Security assessment and quarterly network scans
Level 3	
Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 credit card accounts/transactions annually	Annual self-assessment questionnaire and quarterly network scans

Table 3: Service provider levels

* Payment gateways are a category of agent or service provider that stores, processes, and/or transmits cardholder data as part of a payment transaction (for example, PayPal). Specifically, they enable payment transactions (e.g., authorization or settlement) between merchants and processors (for example VisaNet endpoints). Merchants may send their payment transactions directly to an endpoint, or indirectly to a payment gateway.Stringent compliancy deadlines

Major card companies are pushing hard on merchants who must adhere to the PCI DSS compliance. Various deadlines have been set and hefty sanctions and fines have been placed for organizations who fail to arrive to the finish line on time. Amongst important deadlines, Visa USA has set:

- March 31, 2007 – The deadline by which level 1 and 2 merchants should demonstrate that they are not storing full track data, CVV2 or PIN data.
- September 30, 2007 – The date by which all level 1 merchants are expected to be fully PCI

DSS compliant.

- December 31, 2007 – The date by which all level 2 merchants are expected to be fully PCI DSS compliant.

Deadlines for compliance may vary between card associations and regions; therefore hesitant merchants and service providers should make the seasoned decision to consult acquirers or card associations for their respective deadlines.

Why is it important for your business to comply?

Though a U.S.-led standard, PCI DSS is a global requirement for all entities handling cardholder data. Not all countries are aware of this, for example, widespread confusion in Australia's banking industry about new compliance measures has led to five breaches during 2006 of the PCI DSS.

It's in the own interest of acquiring banks to ensure their merchants are aware and compliant to PCI DSS. The reason is quite logical – acquiring banks are the main actors that build up the line of trust between card companies and merchants – consequently they are also the ones that end up directly in the line of fire of credit/debit card companies whenever one or more of their merchants suffers a breach. To maintain a successful and healthy business relationship with card companies, acquiring banks must ensure that their merchants are adequately protected; and PCI DSS is the tool that gauges cardholder data security on the merchants side.

Similarly, merchants and service providers are expected to demonstrate their level of compliancy to PCI DSS. This helps maintain a healthy business relationship with acquiring banks and avert non-compliance liabilities,

What are the consequences of not complying?

Card companies may impose fines on their member banking institutions when merchants are found to be non-compliant with PCI DSS. Acquiring banks may in turn contractually oblige merchants to indemnify and reimburse them for such fines. Fines could go up to $500,000 per incident if data is compromised and merchants are found to be non-compliant. In the worst case scenario, merchants could also risk losing the ability to process customers' credit card transactions.

Businesses from which cardholder data has been compromised are obliged to notify legal authorities and are expected to offer free credit-protection services to those potentially affected.

There may be other consequences besides the fines. Cardholder data loss, whether accidental or through theft, may also lead to legal action being taken by cardholders. Such a step will result in bad publicity, which may in turn lead to loss of business.

What solutions does GFI provide to help you meet PCI requirements?

Technology solutions can be implemented to automate some of the tasks you need to undertake to satisfy PCI requirements. These solutions allow you to monitor adherence to the standard and to alert you when unauthorized events related to cardholder data take place. GFI provides software tools which help you do just this.

GFI EventsManager, GFI LANguard Network Security Scanner (N.S.S.) and GFI EndPointSecurity are three award-winning network security products from GFI. Through auditing, monitoring, reporting and alerting these products can help you address multiple sections in nine of the 12 PCI requirements, as illustrated in Table 4 below.

PCI DSS REQUIREMENTS	GFI EventsManager	GFI LANguard N.S.S.	GFI EndPointSecurity
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	•	•	
3. Protect stored cardholder data	•		•
4. Encrypt transmission of cardholder data across open, public networks			
5. Use a regularly update anti-virus software or programs		•	
6. Develop and 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 and monitor all access to network resources and cardholder data	•	•	
11. Regularly test security systems and processes	•	•	•
12. Maintain a policy that addresses information security for employees and contractors			

Table 4: PCI DSS Requirements

GFI EventsManager

Events data analysis is directly specified in requirement 10 (Table 4 above) but it is also good practice for any organization to monitor events.

In a typical network environment, events data is distributed, voluminous and cryptic. Event analysis tools supplied by default within most operating systems offer only the most basic of features. As a result, administrators have no means of being alerted when particular important or problematic events are logged, such as the unauthorized access of cardholder data. Events browsing and filtering tools provided by these tools have very limited search and filter capacities.

GFI EventsManager is a complete log management solution which overcomes all these hurdles, allowing you to centralize events, automate event collection, receive alerts and issue investigative reports. When collecting events, GFI EventsManager's inbuilt rule sets process the events in order to classify them and trigger alerts/actions accordingly. One of the default rule sets provided is specifically targeted towards event classification based on PCI requirements. Event analysis can be carried out through the built-in events browser; queries can also be created and executed to retrieve and analyze specific events.

Through GFI EventsManager businesses can ensure that all events related to cardholder data are being constantly monitored. For more information and to download the product, visit http://www.gfi.com/eventsmanager/.

GFI LANguard Network Security Scanner

Vulnerability management is central to requirements 5 and 6 (Table 4 above). However, being able to detect vulnerabilities in various areas covered by other requirements is of utmost importance.

GFI LANguard Network Security Scanner (N.S.S.) addresses the three pillars of vulnerability management: security scanning, patch management and network auditing in one integrated solution. GFI LANguard N.S.S. scans the entire network for over 15,000 vulnerabilities, identifies all possible security issues and provides administrators with the tools they need to detect, assess, report and remediate any threats before hackers do.

Having to deal with problems related to vulnerability issues, patch management and network auditing separately, at times using multiple products, is a major concern for administrators. Not only do they have to install, learn to use and manage multiple solutions but their time is mostly spent trying to understand where the problems are instead of actually addressing the threats that may be present. Using a single console with extensive reporting functionality, GFI LANguard N.S.S.'s integrated solution helps administrators address these issues faster and more effectively.

Through GFI LANguard N.S.S. businesses can ensure that cardholder data is maintained in a

secure environment. For more information and to download the product, visit http://www.gfi.com/lannetscan/.

GFI EndPointSecurity

Protecting stored cardholder data, requirement 3 (Table 4 above), is a key requirement of the PCI data security standard. Ensuring that this data does not fall into the wrong hands is crucial.

It is a well known fact that mass storage devices, such as USB pen drives, have grown in popularity in the last few years. They are easy and fast to install, capable of storing huge amounts of data, and small enough to carry in a pocket. With no security mechanism in place, copying all cardholder data onto such a device can be done easily and swiftly.

GFI EndPointSecurity is the security solution that helps you maintain data integrity by preventing unauthorized transfer of content to and from the portable storage devices. Through its technology, GFI EndPointSecurity enables you to allow or deny access to a device as well as to assign (where applicable) 'full' or 'read only' privileges over a particular device or to a local or Active Directory user/group. With GFI EndPointSecurity you can record the activity of all portable devices being used on your network computers, including the date/time of usage and by whom the devices were used.

Through GFI EndPointSecurity businesses can ensure that cardholder data is not being copied on to unauthorized storage devices. For more information and to download the product, visit http://www.gfi.com/endpointsecurity/.

GFI ReportCenter

GFI ReportCenter is a centralized reporting framework that allows you to generate various reports using data collected by each one of the GFI products. GFI EventsManager, GFI LANguard N.S.S. and GFI EndPointSecurity all have ReportPacks which plug into the GFI ReportCenter framework.

These ReportPacks are powerful reporting companion tools with numerous pre-configured reports. They also include a comprehensive set of features such as report scheduling, report export and automated report distribution via email. Reports generated through the ReportPacks are valuable to businesses when assessing the effectiveness of their PCI compliance program. For more information and to download a ReportPack, visit http://www.gfi.com/reportcenter/.

Incentives

It is in the interest of organizations holding credit card data to comply with the PCI Data Security Standard. It is also within the interest of banks to ensure that merchants comply.

Banks could offer incentives to merchants to comply by offering them GFI network security product licenses as part of the signing on deal. They could also provide additional services, such as technical expertise on the GFI products. This would be a win-win situation as

merchants can achieve safety of mind in being compliant to the PCI DSS, besides having all the other benefits provided by GFI's products. Banks can also achieve safety of mind knowing that the merchants whom they have authorized to accept credit card payments have taken a big step towards achieving compliance.

Conclusion

Companies are constantly at risk of losing sensitive cardholder data. Such a loss will result in fines, legal action and bad publicity. This will in turn lead to loss in business. Achieving compliance to the PCI Data Security Standard should be high on the agenda of organizations who carry out business transactions involving the use of credit cards.

Implementing software tools for log management, vulnerability management, security scanning and endpoint security will go a long way towards helping you achieve compliance. GFI's network security products can assist you in doing just this.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, Adelaide, Hamburg and Cyprus which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.

Sources

CreditCards.com (2006) *Credit Card Industry Facts and Personal Debt Statistics* available from: http://www.creditcards.com/statistics/statistics.php (last cited 29 Dec 2006).

U.S. Census Bureau (2006) *Quarterly retail e-commerce sales 2nd quarter 2006* available from: http://www.census.gov/mrts/www/data/html/06Q2.html (last cited 29 Dec 2006).

Federal Trade Commission (2006) *Consumer Fraud and Identity Theft Complaint Data January – December 2005.*

United States Postal Service *Identity Theft: Stealing Your Name and Your Money* available from: http://www.usps.com/postalinspectors/IDtheft2.htm (last cited 29 Dec 2006).

Bednarz A. (2006) *Online merchants will lose $3 billion to fraud in 2006*, Network World, Inc. available from: http://www.networkworld.com/news/2006/111406-online-merchants-fraud.html?nlhtsec=1113securityalert2 (last cited 29 Dec 2006).

Marlin S. (2005) *Customer Data Losses Blamed On Merchants And Software*, CMP Media LLC available from: http://www.informationweek.com/showArticle.jhtml?articleID=161601930 (last cited 29 Dec 2006).

Ward M. (2005) *Web shops face tighter security*, BBC available from: http://news.bbc.co.uk/2/hi/technology/4449759.stm (last cited 29 Dec 2006).

Evers J. (2005) *Credit card breach exposes 40 million accounts*, CNET Networks, Inc. available from: http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html (last cited 29 Dec 2006).

Extended Retail Solutions (2006) *Fighting spyware and retail identity theft*, GDS Publishing Ltd. available from: http://www.extendedretail.com/pastissue/article.asp?art=25770&issue=147 (last cited 29 Dec 2006).

Schneier B. (2005) *Schneier on Security: Visa and Amex Drop CardSystems*, Schneier.com available from: http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html (last cited 29 Dec 2006).

Harris Interactive (2005) *Global Consumer Attitudes and Behaviors Toward Data Security*, Visa International.

Krebs B. (2006) *ID Thieves Turn Sights on Smaller E-Businesses*, The Washington Post available from: http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html (last cited 29 Dec 2006).

Cybertrust (2006) *PCI Merchant & Service Provider Levels* available from:

http://www.cybertrust.com/solutions/compliance_governance/pci_compliance/pci_levels/ (last cited 29 Dec 2006).

MasterCard *Merchant Levels Defined* available from: http://www.mastercard.com/us/sdp/merchants/merchant_levels.html (last cited 29 Dec 2006).

Pauli D. (2006) *Australian Compliance Confusion Leads to Security Breaches*, CXO Media Inc. available from: http://www2.csoonline.com/blog_view.html?CID=25049 (last cited 29 Dec 2006).

Wells Fargo *Merchant Services - Payment Card Industry (PCI) Data Security Standards FAQs* available from: https://www.wellsfargo.com/biz/help/merchant/faqs/pci#Q24 (last cited 29 Dec 2006).

PCI Security Standards Council (2006) *Payment Card Industry (PCI) Data Security Standard* (Version 1.1) available from: https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.