



PCI Data Security in the Parking Industry

White Paper

Disclaimer

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Digital Payment Technologies Corporation.

No patent liability is assumed with respect to the use of the information contained herein. Neither is any liability assumed for damages resulting from the use of the information contained herein.

The Digital brandmark is a Service Mark of Digital Payment Technologies Corporation. © Copyright 2008 Digital Payment Technologies™ Corporation. All rights reserved.

Contents

Executive Summary	7
The High Cost of Poor Data Security	9
PCI Data Security Standard Overview	10
Types of Businesses Impacted	11
Self-Assessment vs. Formal Assessment	14
The Path to Compliance	16
Case Study – An American University	18
About Digital Payment Technologies Corp.	20
References	21

Costs resulting from credit card breaches exceed \$2 billion annually.

Executive Summary

Parking operators, municipalities and universities are under increasing pressure to ensure proper data security policies and technologies are in place to protect consumer credit card information. Poor credit card data security policies and outdated technologies are costing North American banks and credit card processors billions of dollars each year. The overall cost to credit card companies, banks, businesses and consumers is staggering. For the banking industry alone, it is estimated that the costs resulting from credit card breaches are over \$2 billion annually.ⁱ

The rippling affect of these costs is being felt by individual businesses as credit card companies impose fines to limit their losses while also protecting their brand image. Avoiding these costs can only be achieved by companies in the parking industry if each business and equipment supplier educates themselves on the credit card industry's Payment Card Industry (PCI) Data Security Standard and the steps required to meet these standards.

The financial impact on the parking industry is just one part of the problem. There is also the loss in consumer confidence in credit cards and the parking facilities and technologies that accept those cards. With competing threats from new cashless payment methods such as PayPal, the credit card industry is beginning to take a much firmer stance with its affiliated Merchants and Service Providers to ensure that credit card data and the credit card name brand are protected.

For many businesses in the parking industry, compliance to the PCI standards is mandatory. Failure to understand and meet the requirements can result in significant fines, and perhaps more importantly, the risk of a security breach and the loss of confidence by the parking public.

The High Cost of Poor Data Security

Criminals have more ways to exploit weaknesses in credit card security.

Credit cards have been around for over 50 years, but with rapid improvements in technology over the last decade, criminals have become more sophisticated in finding ways to exploit weaknesses in credit card security. Criminal methods such as social engineering, phishing and skimming are becoming commonplace in the public eye as these methods are reported in an increasing number of newspaper reports on credit card fraud. Data from the Privacy Rights Clearinghouse, a non-profit consumer information source, reports that over 225 million personal records have been compromised in the U.S. between January 2005 and May 2008.ⁱⁱ

One of the more well-known cases of security fraud was revealed in early 2007 when Massachusetts-based TJX, a \$17.4 billion corporation that operates the T.J. Maxx and Marshall retail chains, reported that over 45.7 million credit and debit card numbers were stolen in a security breach lasting 18 months. Subsequent reports from insiders have indicated that the amount of credit card numbers stolen could reach over 200 million with Forrester Research estimating that the total cost to the company could escalate to over \$1 billion over a five-year period. These estimates do not include potential lawsuit liabilities.ⁱⁱⁱ

The total costs resulting from a credit card security breach stem from several areas, the primary being:

- Fines
- Consultants
- Security upgrades
- Legal action
- Marketing to re-assure customers

One of the largest costs is the fines imposed by the credit card companies. These fines have been escalating over time as each credit card company attempts to impose more pressure on merchants and service providers. Each credit card company has its own fine structure for a breach, with Visa having the highest fines \$50,000 for the first violation, \$100,000 for the second violation and a third violation fine at management's discretion.^{iv} These costs escalate even more if there is a failure to immediately notify Visa of the breach. These additional fines range from \$100,000 to \$500,000 per incident, depending on whether the merchant or service provider compromised is compliant at the time of the incident.^v In 2006, Visa issued \$4.6 million in fines, up from \$3.4 million in 2005.^{vi}

Average cost of a security breach is \$182 per customer record.

As the TJX example illustrates, the overall cost of a breach to businesses and the industry as a whole is obviously much higher. In 2006, the Ponemon Institute conducted a benchmark study of 31 different companies to determine the actual cost of a security breach. These companies experienced costs that averaged \$4.8 million per incident based on an average of 26,300 records lost. The study found that the average cost of a breach was \$182 per lost customer record. This number was then

broken down by direct incremental costs such as legal fees (\$54 per lost record), productivity costs for lost employee time (\$30 per lost record) and customer opportunity costs from customer turnover (\$98 per lost record).^{vii}

Given these high costs associated with poor data security, it is imperative for businesses within the parking industry to understand the PCI Data Security Standard and the responsibilities of each business under this standard.

PCI Data Security Standard Overview

The first comprehensive response to protect credit card data was Visa's Cardholder Information Security Program (CISP) that was established in 2001. The program outlined a broad number of guidelines to businesses to promote an understanding of basic data security fundamentals and to recommend enhancements to existing security programs. In response, MasterCard developed a similar program called the Site Data Protection Program (SDPP) and American Express developed the American Express Data Security Standard (AEDSS).

While the goals of these programs were similar, it became difficult for businesses operating with all three cards to support the different standards. The credit card companies then decided to consolidate their ideas and form version 1.0 of the Payment Card Industry (PCI) Data Security Standard in 2004. In September 2006, the group was expanded to include Discover Financial Services and JCB. All five organizations then announced the formation of the PCI Security Standards Council (PCI SSC) and the release of version 1.1 of the PCI standards. The council was established to cover a wide range of areas that included the management of the ongoing evolution of the PCI standards and the establishment and maintenance of industry-level-approved processes for qualified security assessors.

PCI Data Security Standard requires the secure storage, processing and transmission of cardholder data.

The foundations of the PCI Data Security Standard are the technical requirements for the secure storage, processing and transmission of cardholder data and the outline of common auditing and scanning procedures. The details of these areas are summarized in the 12 general requirements highlighted below:

PCI Data Security Regulations^{viii}

Build and Maintain a Secure Network

1. Install and maintain a network firewall to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update antivirus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

10. Track and monitor access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Following each of these regulations are numerous sub-sections detailing how businesses can ensure data security is maintained. These details include the minimum encryption methods to be used, the proper setup of a firewall, the types of characters that must be included in a password and the amount of credit card information that may be displayed on a receipt.

Many U.S. states have now expanded upon the groundwork laid by PCI. As of August 2007, 35 states have implemented their own credit card security laws. A key component of all of these laws is the requirement that businesses have a legal obligation to notify consumers if there is a security breach. Legislation, such as a bill proposed in Massachusetts in February 2007, has also been considered to expand the scope of the penalties by requiring businesses subject to a breach to pay the full costs borne by credit card companies to issue new cards to the public.^{ix}

Types of Businesses Impacted

Another component of the PCI standards is an outline of the minimum requirements that must be met by the three business categories. The three categories and their definitions are:

Merchants

Companies that accept credit card transactions for payment. In the parking industry, these would include private parking operators, universities and municipalities.

Service Providers

Companies that facilitate the processing of credit card transactions. This category would primarily apply to the various merchant banks such as

Chase Paymentech and credit card processor gateways such as Authorize.Net.

Application Vendors

Companies that manufacture equipment that accept credit cards as a method of payment. These would include multi-space parking meters, gated systems, transit fare boxes and pay-by-foot equipment.

Each group must comply with the standards or face significant fines by the credit card company in the event of a security breach. However, proof of compliance may be acquired through either a self-assessment or a formal assessment by an independent Qualified Security Assessor (QSA). Each credit card company may have slightly different standards when an assessment is required, but Visa has the most commonly held standards for each category. Visa's standards for each category are outlined in the following tables:^x

Each group must comply with the standards or face significant fines.

Merchants	Level 1	More than 6 million transactions annually
	Level 2	1 million to 6 million transactions annually
	Level 3	20,000 to 1 million transactions annually
	Level 4	Less than 20,000 transactions annually
<ul style="list-style-type: none"> Level 1 – requires an annual formal assessment by a QSA Levels 2/3/4 – require an annual self-assessment All levels require a quarterly network scan 		

Service Providers	Level 1	Gateway / Processor
	Level 2	More than 1 million transactions annually
	Level 3	Less than 1 million transactions annually
<ul style="list-style-type: none"> Level 1 – those who aggregate customers for the processing of credit card transactions Levels 1 and 2 – require a formal assessment by a QSA 		

Application Vendors	Any software application that accepts credit cards is classified as an Application Vendor	
	<ul style="list-style-type: none"> A third-party validation program is available Compliance to the standard is currently voluntary 	

Requirements for application providers fall under a subset of the PCI Security Program called Payment Applications Best Practices (PABP). PABP was originally created and overseen by Visa as its research confirmed that vulnerable payment applications are the leading cause of compromise incidents, particularly among small merchants.^{xi} In April 2008, the PCI SSC assumed responsibility for the program and released the Payment Applications Data Security Standard (PA-DSS) in an effort to update the standard and assist in promoting the validation of secure payment applications everywhere.

Key components of this announcement was an outline as to how vendors validated under PABP can migrate to the new standard and the increased requirements for those vendors who have failed to validate to this point. All vendors who have successfully validated under PABP versions 1.3 or 1.4 have been grandfathered to the new standard and will be listed as successfully validated on the new PCI SSC list. Each of these companies must then undergo a PA-DSS assessment anywhere between 18 and 24 months from the date of the initial publication of the PCI SSC list, depending on the PABP version of original validation.

Each payment brand will determine as to whether PA-DSS standard will be mandatory for all payment application providers; however, Visa has already outlined a series of mandates to ensure compliance is enforced. These mandates include:^{xii}

- January 1, 2008: New merchants are prohibited from certifying new payment applications that are known to be vulnerable.
- July 1, 2008: VisaNet Processors (VPN) and agents must only certify new payment applications to their platforms that are PA-DSS compliant.
- October 1, 2008: Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PA-DSS compliant applications.
- October 1, 2009: VPNs and agents must decertify all vulnerable payment applications.
- July 1, 2010: Credit card processors must ensure their merchants and VPNs and agents use only PA-DSS compliant applications.

While these mandates accept a vendor's self-assessment as compliance, many merchants and credit card processors are informing payment application vendors that successful completion of an audit by a QSA is mandatory to ensure protection from the potential liability of using vulnerable applications. Only those vendors who have successfully completed an audit will appear on the PCI DSS list as validated payment applications under PA-DSS.

The industry may expect PCI DSS and the credit card companies themselves to also make a third-party audit compulsory at a later date if the number of vulnerable applications appearing continues to grow. In a November 2007 press release, Michael E. Smith, senior vice president, payment system risk at Visa Inc., expressed his frustration with the lack of response by application vendors by saying: "Criminals are targeting certain versions of software because of their known security gaps. Some versions of software in use today are known to store the full content of the magnetic stripe, PIN data or security codes contrary to Visa rules and the PCI Data Security Standard."^{xiii}

The key requirement under PA-DSS is that payment applications must not retain Track 2 or Card Verification Value (CVV2) data. Track 2 data is the encoded personal information stored on the magnetic stripe of a credit card and the CVV2 number is the three-digital card verification number stored on the back of your credit card. PA-DSS also enforces the guidelines for password levels to be maintained, data encryption levels to be put in place and the amount of credit card data displayed on

You must look closely at each business to determine how they are classified.

consumer receipts.

While each of the three business categories and their requirements may seem fairly straightforward, one must look closely at each business to confirm how they are classified. For example, many Application Vendors in the parking industry also act as Service Providers. These companies aggregate credit card data from multiple companies and transmit it through an online gateway and out to a credit card processor. By doing so, equipment vendors are Level 1 Service Providers requiring a formal assessment by a QSA. Businesses that use equipment without ensuring it is PCI compliant are accepting a high level of risk.

Key questions businesses can ask to determine what categories are operating within their business network include:

1. What companies and equipment are involved in storing, transmitting and/or processing credit card data?
2. How are these companies categorized?
3. What PCI level must each of them meet?
4. Are these companies PCI compliant as a result of a formal assessment by a QSA or is the company only providing a self-assessment?

The question as to whether a self-assessment is enough to provide security assurance is quickly becoming one of the biggest issues a business faces when reviewing the PCI standards and requirements. In answering this question, it is helpful to understand the differences between a self-assessment and a formal assessment and when each approach may be required.

Self-Assessment vs. Formal Assessment

A self-assessment involves reviewing PCI regulations, completing an online questionnaire to validate that the regulations are being met and then the performance of an online computer scan of the businesses' network. In February 2008, PCI DSS updated the questionnaires to include four unique forms addressing various business scenarios. As a sign of the mandate to raise the bar for merchants, service providers, and application vendors, one questionnaire has gone from 11 to 226 questions.^{xiv}

These questionnaires and computer scans can be very helpful in evaluating your current status, as the PCI security scans alone provide Merchants and Service Providers with invaluable information concerning their network system to identify issues such as misconfigurations of Web sites and applications as well as IT infrastructures with Internet-facing IP addresses. Businesses need to be careful not to solely rely on these self-assessments and security scans when evaluating their security status as the implications of an incorrect evaluation can be costly.

Any business that experiences a credit card security breach is subject to a review by a QSA and the assessment of fines if it is determined the self-assessment was answered incorrectly. Given the potential risks involved in having a self-assessment incorrectly answered, many businesses are opting for a formal assessment process even when not required to do so. These same businesses are also not accepting self-

Formal assessments provide the highest level of assurance that an organization is compliant.

assessments as proof of compliance from the Service Providers and Application Vendors they work with. Businesses are now making it an internal requirement that all Service Providers and Application Vendors used become PCI compliant through a formal assessment by a QSA.

A formal assessment process by a QSA provides the highest level of assurances that a Merchant, Service Provider or Application Vendor is PCI compliant. A list of QSAs may be found on the PCI Security Standards Council Web site (<http://www.pcisecuritystandards.org>). It is recommended that several QSAs be contacted before choosing one that is best suited to your business needs. The flexibility and costs of each assessor can vary greatly.

Once an assessor has been selected, it is recommended that they conduct a pre-assessment on your business. This pre-assessment will help determine the specific areas that need to be addressed and provide you with a roadmap for corrective action. Surprising to many, there have been no reported cases of a business ever passing the pre-assessment. Based on statements made by various QSAs, evaluations of fewer than 50 percent achievement of the PCI standards are common.

With the pre-assessment roadmap in hand, businesses may make the necessary changes to their business' security policies and technologies to ensure compliance. These changes can involve items such as establishing proper firewall protection, staff training and documenting new internal procedures and operating standards. In the case of equipment, some legacy systems will be unable to be upgraded to the latest standards under PCI. Assessors have the discretion to outline "compensating controls" for this equipment to protect the credit card data and to avoid the need to completely replace existing systems.

Once a formal assessment takes place, the assessor will produce a Report on Compliance (ROC) to validate that a business has met the standards and is PCI compliant. Other businesses can then confirm which companies are compliant by reviewing lists of compliant companies on credit card company Web sites. An annual formal assessment is then required to remain on these lists as a PCI compliant vendor.

Preventative measures cost only four percent of the cost of a security breach.

Many businesses are hesitant to take the first steps towards a formal assessment because of the additional costs involved, which can be as high as \$100,000 for a Merchant. In 2007, Visa reported that only 36 percent of Level 1 Merchants requiring a formal assessment are actively working toward compliance.^{xv} While it is true that the cost of a formal assessment and the work required to successfully complete one can be high, the statistics from the Ponemon Institute reveal that the cost of new preventative measures averages only four percent of the total costs of a breach.^{xvi} Given the high potential cost of a breach, the extra step of having a formal assessment can prove to be a relatively small and worthwhile investment to confirm that proper security standards are in place.

The Path to Compliance

The path to achieving PCI compliance can be confusing, but the following 10 steps can serve as a general guide to get any Merchant, Service Provider or Application Vendor started:

1. Start Now

While the PCI Data Security Standard is well documented and readily available on the PCI Security Council Web site (http://www.pcisecurity-standards.org/pdfs/pci_dss_v1-1.pdf), it can take a business months to make all the necessary changes to meet compliance. As the pressure and potential fines from the credit card companies and State privacy laws mount, it is in a business' best interest to start on the path to compliance immediately.

2. Assign a Company Lead

Like any project, it is best to have a single point person who can take the lead in understanding the requirements, establish a timetable, liaise with the various departments and keep everyone on track. Given the technical nature of the PCI standards, this lead is typically a Chief Information Officer or an IT department head.

3. Undertake a Self-Assessment

Determine where your business fits under the PCI guidelines and conduct a self-assessment to find out how you are positioned. As mentioned, these self-assessments will likely not capture everything, but they will serve as a starting point to determine how high a mountain you need to climb to be PCI compliant.

4. Take an Inventory

Beyond just your internal systems, take stock of all equipment and Service Providers being used within your business network that are used to accept or process credit card data. These would include access control equipment, multi-space parking meters, single head parking meters, and online permit systems.

Contact all of these third-party companies to find out their position under PCI and determine if they have taken the proactive steps to be validated as PCI compliant by a QSA. This validation can be confirmed by reviewing the lists of PCI compliant Merchants, Service Providers and Application Vendors posted on the Visa (http://usa.visa.com/merchants/risk_management/cisp.html) and MasterCard (<http://www.mastercard.com/us/sdp/index.html>) Web sites. At a minimum, Application Vendors have to be able to provide a detailed PABP User Implementation Guide that outlines how the equipment addresses each of the PABP requirements, even if they have only completed a self-assessment.

5. Make Adjustments

With the results of your self-assessment in hand, take action to make the necessary adjustments to your business technologies and policies.

For some businesses, the requirements outlined are so broad that it may be more economical to jump to the next step and engage a QSA who can help define exactly what is required.

6. Engage a QSA

Third-party validation of your security status is the best way to ensure compliance. All QSAs posted on the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm) may be engaged to provide assessment services. Evaluate several QSAs before selecting one that best meets your needs. An evaluation should include reference checks with businesses of a similar size that have used the assessor. References can provide you with a better idea of the assessor's approach, time requirements and flexibility to keep the assessment costs to a minimum.

7. Complete a Pre-Assessment

A pre-assessment conducted by your QSA can save a lot of time and money by outlining a specific roadmap to achieving compliance before beginning the formal assessment process. The pre-assessment is about one-eighth of the total cost of a formal assessment.

A pre-assessment can save a lot of time and money.

8. Remediation

The pre-assessment will produce a list of remediation items that can be undertaken to meet the standards. Remediation items can include changes to network configurations, hiring policies and physical office security. Depending on the results of the pre-assessment, the completion of these remediation items can take months.

9. Assessment

The PCI and PABP validation processes will take place over several days and usually requires booking an assessment months in advance as QSAs are in high demand. Once a formal assessment has been successfully completed, the QSA will complete their ROC and submit it to the credit card companies for posting on their Web sites.

10. Annual Review

Successfully becoming PCI compliant does not end with the completion of an assessment. The standards are evolving specifications that change regularly and require each Merchant, Service Provider and Application Vendor to re-validate annually. Companies that fail to re-validate or to meet the latest standards will be highlighted on the Visa and MasterCard Web sites.

Case Study – An American University

Much of today's media attention on data security focuses on large retailers such as TJX; however, this does not mean that parking operations are immune to these types of issues or the financial implications stemming from a lack of proper security measures. The parking department of a major U.S. university, hereafter referred to as the University Parking Department (UPD) so as to keep its anonymity, shares the story of a breach it faced, the results, and the steps it took. The UPD chose to share its story to highlight the impact of poor data security within the parking industry and the proper mechanisms used to address it.

The UPD is a fairly typical university parking operation with a combination of short- and long-term parking lots and garages, multi-space parking meters, in-lane parking equipment and a Web portal accepting online permit sales with credit cards by Visa, MasterCard and American Express. At the start of 2005, the number of credit card transactions within the parking facilities was over 48,000 annually.

Later in 2005, it was discovered that UPD's computer system had been compromised resulting in unauthorized access. The affected server was part of the UPD's point-of-sale system and was used specifically to process credit card authorizations using a card swipe and dial-up modem. The university's IT Security Office identified the server attack as a result of network monitoring and investigation processes that had been implemented on campus. Specifically, network monitoring identified inappropriate traffic originating from the system in question.

The IT department reacted quickly to isolate the server and shut down the affected system. Use of the malicious files uploaded during the compromised period would have permitted an attacker to access the information contained in the log files. However, a review of the access times of the log files indicated that none of the files were accessed during the intrusion. Therefore, no cardholder data – including any track data – that was present in the log files was viewed or otherwise accessed during the compromised period.

Ultimately, the fact that card data could have been accessed was considered a breach by the credit card companies and this elevated the UPD under the PCI Data Security Standard from a Level 3 Merchant to a Level 1 Merchant, thereby requiring a mandatory formal assessment. The UPD immediately stopped the support of credit cards on all parking related equipment and services and then hired a forensic scientist to review the existing computer systems and provide recommendations for improvements.

In the coming months, the UPD took remedial steps by engaging a local network and security technology company to assist in addressing security issues with the existing technology infrastructure and worked with a QSA to perform the formal assessment as required under the PCI Data Security Standard.

The QSA conducted its formal assessment in early 2006 and issued an ROC validating that the parking department had met all the mandatory PCI data security requirements. Specific changes undertaken by the

UPD as a result of the assessment and requirements stemming from the ROC included:

- Network software and firewalls were all upgraded to isolate the point-of-sale system from both the internal and external networks
- Complex passwords were implemented for all network users
- Facility entry controls, policies and procedures were established
- Controls over stored data were implemented
- Data access and storage restrictions were established
- Databases containing credit card information were segmented from the network
- Specific facilities containing credit card data had locks installed
- Background check policies and procedures were updated
- Additional security cameras installed
- Reconfigured workspaces to provide more secure processing areas
- Credit card incident policies and procedures were established
- New multi-space parking technologies that met the PCI standards were sourced so that credit card acceptance could resume in parking lots and on-street spaces

The resulting costs from this breach have been estimated at almost \$50,000.

The costs resulting from this breach have been estimated at almost \$50,000 with \$8,000 in legal assistance and IT consultants, \$6,500 for the assessment and \$35,000 in fines from the credit card companies. Despite these steep costs, the UPD recognizes the financial implications could have been far worse or more sensitive credit card information could have been stolen, had the breach not been caught early.

Moving Forward

While the incident was certainly something the UPD would rather have avoided, the recovery process has proved to be invaluable in helping determine what steps are necessary to protect customers' sensitive information. Whether through the Internet, in the field, at attended parking facilities or by cell phone, customers want to be able to pay by credit card, so the UPD must adapt its systems to accommodate market forces while providing strict control of sensitive cardholder information. Since the breach was first reported, UPD has begun the process of rebuilding its payment systems. Each vendor wanting to provide equipment or services is required to disclose their PCI status and provide documentation supporting that status. New contracts that are written include specifications relating to PCI and PABP that are flexible enough to allow for future changes in industry standards.

Finally, the UPD and the university's Department of Public Safety have invested more heavily in the human resources necessary to keep pace with the ever changing IT environment. Each revenue control equipment purchase necessitates close coordination with in-house IT staff as well as the university Treasurer's office and IT department. Even with these changes and the infusion of additional financial resources to provide more security technology and staff, the UPD recognizes that adopting new operational procedures is the key to ensuring a safe

credit card environment. It also happens to be the most difficult aspect of change, shifting the prevailing way of thinking – we’ve always done it that way.

The end goal for the UPD calls for a robust revenue control system that simultaneously offers customers choice and security. While the incident described here was unfortunate, the UPD is stronger today than before and will be more secure as time passes.

Conclusion

Data security is a critical part of every business that accepts credit cards.

Data security is a critical part of every business that accepts credit cards. The financial and negative public relations implications of failing to address this issue are growing, so parking operators, municipalities and universities must start paying closer attention to ensuring their operations and the equipment they use meet the latest PCI standards. The best approach every organization can take is to be proactive in understanding the PCI regulations, how these regulations affect their operations and the actions that must take place to ensure that proper data security standards are in place for the short- and long-term.

About Digital Payment Technologies

Digital Payment Technologies (DPT) is an innovative leader in the design, manufacture and distribution of electronic multi-space parking meters, parking management software, and online services for the multi-billion-dollar parking industry. The company’s products provide complete financial tracking, control and reporting for parking revenue collected by municipalities, universities, parking management companies, and national parks, from customer payment through to bank deposit.

DPT successfully completed its first PCI Compliance audit as a Level 1 Service Provider in April 2007 and all DPT products were validated under PABP in December 2007. DPT and its products continue to receive an annual audit by a QSA to ensure the latest PCI standards are met.

Digital Payment Technologies

330–4260 Still Creek Drive
Burnaby, BC
V5C 6C6

888.687.6822 | digitalpaytech.com

References

- ⁱ Joseph Pereira, "Bill Would Punish Retailers for Leaks in Personal Data," *Wall Street Journal*, February 22, 2007 Page B1
- ⁱⁱ Privacy Rights Clearinghouse, "A Chronology of Data Breaches," <http://www.privacyrights.org/ar/ChronDataBreaches.htm#1>
- ⁱⁱⁱ Joseph Pereira, "How Credit-Card Data Went Out Wireless Door," *Wall Street Journal Online*, May 4, 2007
- ^{iv} First National Merchant Solutions, PCI Data Security Standards, "The Payment Card Industry Data Security Standard," http://www.firstnationalmerchants.com/ms/html/en/pci_compliance/pci_data_secur_stand.html
- ^v Visa, "Cardholder Information Security Program," http://usa.visa.com/merchants/risk_management/cisp.html
- ^{vi} Visa, "Visa USA Pledges \$20 Million in Incentives to Protect Cardholder Data," December 12, 2006
- ^{vii} The Ponemon Institute, "2006 Annual Study: Cost of a Data Breach. Understanding Financial Impact, Customer Turnover and Preventative Solutions," April 2007
- ^{viii} PCI Data Security Council, "Payment Card Industry (PCI) Data Security Standard, Version 1.1.1," September 2006, Page 1
- ^{ix} Joseph Pereira, "Bill Would Punish Retailers for Leaks in Personal Data," *Wall Street Journal*, February 22, 2007 Page B1
- ^x Visa, "Cardholder Information Security Program," http://usa.visa.com/merchants/risk_management/cisp.html
- ^{xi} Visa, "Visa Mandates Use of Security Payment Software in the United States," November 8, 2007
- ^{xii} Visa, "Visa's Payment Application Best Practices adopted as Security Standard," April 15, 2008
- ^{xiii} Visa, "Visa Mandates Use of Security Payment Software in the United States," November 8, 2007
- ^{xiv} PCI Security Standards Council, "PCI Security Standards Council Issues Updated Self-Assessment Questionnaire," February 6, 2008
- ^{xv} Visa, "Visa USA Pledges \$20 Million in Incentives to Protect Cardholder Data," December 12, 2006
- ^{xvi} The Ponemon Institute, "2006 Annual Study: Cost of a Data Breach. Understanding Financial Impact, Customer Turnover and Preventative Solutions," April 2007