

Profiting from PCI

Researched and authored by Wendy Atkins, freelance journalist, on behalf of ACI Worldwide

October 2006



Every year, the financial services industry faces new challenges and new threats as it races to keep up-to-date with the latest business, technology and security pressures. But it's not all bad news; each set of pressures brings with it its own opportunities, and organisations are looking at ever-more creative ways of harnessing them.

With organisations involved in card payments entering the latest stage on the road to Payment Card Industry (PCI) Data Security Standards compliance, we examine the current state of play and ask how organisations can turn 'yet another level of compliance' into a real opportunity that benefits businesses and customers alike.

Following several years of high-profile stories about payment card security breaches, a small percentage of consumers has lost confidence in payments cards. This is unfortunate because it comes at a time when most people in the developed world have at least one bank account, and payments cards are becoming the most popular ways of making transactions.

For example, during 2005, in the United Kingdom alone, only 5 percent of retail purchases were made by cheque, compared with more than 60 percent by debit or credit card, according to the country's payments organisation, APACS. And in France, where take-up of credit and debit cards has traditionally been slower than in the United Kingdom, there has been a marked increase in the number of card payments. In 2005, payments made by Cartes Bancaires cards reached €236.8 billion, representing more than a quarter of household expenditure in the country.

A Long Time Coming

As payments cards become increasingly popular, the industry must work to maintain and build consumer confidence in card-based transactions. PCI is one of the latest initiatives to deal with the challenges presented by increasingly sophisticated criminals.

PCI has existed in some form for around five years, so it should not be dismissed as a simple knee-jerk reaction to the challenge of ensuring payment security. Initially started by Visa in 2001, it was originally called the Cardholder Information Security Program (CISP). In this guise, it aimed to address the increasing incidence of hackers accessing e-Commerce sites and stealing cardholder information and other data. In the early days, breaking into sites was simply a technical process carried out by hackers to cause maximum embarrassment to merchants by hacking card data and publishing it on the Internet to show how clever they were. The hackers certainly scored a PR jackpot when they hacked the cards of big names — such as Bill Gates — and posted them on a site.

The PCI Standard aims to create cardholder confidence in the payment card system by ensuring their card details are secure at every stage of the transaction process. This is especially important given that the stakes are now higher, with hacking becoming much more harmful. The PR win of hacking Bill Gates' information has given way to card data being used for fraudulent card-not-present (CNP) transactions or being sold to national organised crime groups. And, although card-present fraud is decreasing, CNP transactions have continued to climb. In the United Kingdom alone, CNP amounted to £183.2 million in 2005, up 21 percent from 2004.

To address the growing — and costly — problem of Internet fraud, MasterCard introduced the Site Data Protection (SDP) scheme in 2004. Also that year, Visa and MasterCard jointly developed and launched PCI, which was later endorsed by American Express, JCB and Discover Financial Services. PCI is based on existing sets of standards, such as BSS 7799, but has been adapted and refined to address the payment industry. PCI is intended to provide a global baseline that all stakeholders across the payment industry should implement as an absolute minimum security measure.

Profiting from PCI

PCI has the backing of all of the major cards players. In September 2006, American Express, Discover Financial Services, JCB, MasterCard and Visa announced the formation of an independent council to manage the development of PCI data security standards.

The council has a fairly wide remit, including developing and maintaining global industry-wide technical data security standards and procedures for use by all payment brands. It has also taken over from MasterCard and Visa the maintenance of lists of approved scanning vendors and qualified security assessors.

As well as developing technical specifications, the organisations behind the PCI standard have also set a series of objectives and deadlines. By 30 June 2007, retailers, financial services institutions and businesses that accept card payments must be compliant with PCI Standards. Those that are not face the threat of losing cardholder data through fraud, leading to substantial brand damage, loss of customers, fines or even being barred from accepting card payments.

The role of PCI has changed over the years in response to the current challenges faced by the payment industry. Initially, it was seen as ensuring that any provider of financial services played a positive role in the payments community by looking after and respecting customer data. However, recent cases of card fraud indicate that its impact really is significant because, at best, a serious attack can result in a loss of consumer confidence in an institution, resulting in a drop in business. At worst, an institution could collapse if it suffered serious security problems.

Businesses are becoming increasingly aware of the standard and the vast majority have assessed what impact the new specifications will have on their operations. Payments processors have taken the lead here, with awareness growing substantially over the past six to 12 months. The next step is for organisations to act to ensure compliance. This means attaining board-level approval to make the necessary changes and implementing new technologies and procedures.

Under Pressure

Merchants and payment processors are taking the threat of such security problems seriously, because it is essential that consumer faith in payment systems is not dented in any way. PCI, which consists of 12 technology audit requirements for securing networks and applications and protecting cardholder data, comes at a time when the industry is

having to counter media criticism and consumer concern about the security of personal financial data.

The PCI requirements cover everything from securing networks and cardholder data, to providing access rules for users and establishing and using procedures that are fully auditable. Initially, PCI protected Internet transactions, an area where consumer confidence had been shaken by much-publicised cases of card fraud. However, it now applies to all organisations that store, process or transmit cardholder data.

“The normal path to attaining PCI-compliance certification is to start with a self-assessment audit using the documentation from one of the payment schemes [e.g., MasterCard or Visa],” said Steve Edwards, head of product management at ACI Worldwide.

Organisations seeking to achieve compliance must initially meet all 12 requirements and then prove they have been met through an external audit, which is carried out by companies accredited by Visa, MasterCard and American Express.

“The normal path to attaining PCI-compliance certification is to start with a self-assessment audit using the documentation from one of the payment schemes [e.g., MasterCard or Visa],” said Steve Edwards, head of product management at ACI Worldwide. “With this completed, a pre-audit survey is performed by an audit company. It will identify what needs to be changed in the current technical and operational environment. The organisation will need to complete these changes before an official audit is done.

“What really helps is to have the technical platforms compliant with certification from one of the payment schemes,” Edwards continued. “Having achieved PCI compliance status, organisations must then undergo a regular audit, along with self-assessment audits. The period between audits depends on the transaction volumes being processed by the service.”

Compliance requirements cover three key areas of the process: the technical infrastructure, the payment applications and many aspects of standard procedures. The PCI guidelines affect every part of the payments value chain. They require merchants to have the security of their key storage and credit card transaction processes audited. This means that, at a minimum, merchants must install and maintain

Profiting from PCI

a firewall, encrypt data transmitted across public networks, use and frequently update antivirus software, assign a unique ID to each person with computer access, and regularly test and monitor access to network resources and cardholder data. For payments processing companies, the PCI Standards include a mandate to implement two-factor authentication systems as a means of securing network access.

“A massive amount of investment and effort is needed,” said Jim Shaffer, senior product manager at ACI.

The Challenges Ahead

To get through the next few months and achieve compliance, businesses face significant challenges because the standards will have an impact on how they operate and the technology they use.

“A massive amount of investment and effort is needed,” said Jim Shaffer, senior product manager at ACI. “All parts of the industry need to look at aspects of interaction with systems that process cardholder data, and everything will have to be tightened up in terms of physical access, storage and usage, as well as software policies and procedures. For some organisations significant changes to the current network architecture will also be required.”

International Focus

PCI affects payments globally, and some countries are closer than others to achieving deadlines. For example, the United States has historically led the way on PCI compliance for several reasons. Initially, U.S.-based Web sites experienced the greatest level of hack attacks and subsequent negative publicity. More recently, they have been hit by fraud attacks. Furthermore, the U.S. market is more mature, especially in the use of the Internet for transaction services such as e-Commerce and banking.

“U.S. merchants have been made nervous by the high-profile stories of data loss,” Shaffer said. “Added to this, half the states have security breach notification laws and merchants have to notify the authorities of any such security breaches. The value of such notifications — in terms of cost and reputation — can be enormous.”

Europe is not far behind the United States, with all markets in the region committed to achieving PCI compliance.

“Progress towards compliance may be accelerated by such considerations as the number of high-volume merchants a market may have or the strength of public awareness about security in general,” said Steve Wilson, head of AIS compliance at Visa Europe. “All markets are seeing a greater degree of focus on information security issues — with pressure coming from the media, governments, the European commission — and recognise the need to respond.”

Germany is playing a leading role in the EMEA region’s movement towards PCI. “The point-of-sale (POS) network provider market is being affected by PCI,” Edwards said. “In fact, the German regulatory body, the ZKA, is already making PCI compliance a requirement. The big U.S. processors are also driving what’s happening in Europe, with the likes of FDI and Total Systems introducing the standards to the Europeans. Because they actively compete with European processors, their continental counterparts have to follow suit.”

Don’t Dismiss PCI

It could be easy for organisations to dismiss PCI as just another challenge to address. For some organisations, it arrives hot on the heels of EMV, so it could even be seen as a necessary evil rather than an opportunity. However, PCI is far more than a technological challenge.

“EMV requires compliance with specifications and standards,” Shaffer said. “PCI goes way beyond this. It brings into question areas such as personal accountability, policies and procedures.”

However, Paul Baker, vice president, advanced payment solutions at MasterCard Worldwide, pointed out, “There are no dissenting voices surrounding what needs to be achieved, and MasterCard is delighted to be working with each country to overcome any domestic issues and ensuring that any risk is managed and mitigated.”

Organisations will need to make changes, and significant investment may be required in order to become compliant. However, “the payment industry, and the merchants, service providers and vendors that store, process or transmit card data, are in general agreement that PCI is a common-sense approach to the threats of data compromise,” Wilson said. “The difficulties lie in raising the issue to an appropriate level of priority, especially in commercial organisations and markets that have only recently invested in EMV chip standards.”

Profiting from PCI

Baker agreed with Wilson and added, “It is unfortunate that data security has not had a high priority with all merchants in the past, so some have more work and expense to correct these issues than others. The cost of undertaking the programmes can be a challenge to some, but there is a growing realisation that the price of not undertaking compliance could be much higher in terms of brand damage.”

Compliance doesn't have to be just about cost and change. There are, in fact, sound business reasons for looking at the coming challenges as opportunities rather than hassles. PCI can also be seen as a chance to establish better and tighter control of the operations of the systems, both in terms of security and performance. The first point is obvious, but what about the second?

All payments organisations have ISO and other standards in place for operations. The requirement for the PCI audit can be used to review these standards with the objectives of integrating them into current procedures as well as improving and extending these procedures.

For example, the requirement to regularly monitor networks is aimed at pinpointing security flaws, but this approach could also be extended to monitor network performance, reliability and contingency. Furthermore, maintaining an information security policy does not only refer to the points in the audit, it could also be used to define the roles in system support and access controls.

PCI provides the opportunity to ensure that issuers have quality systems and processes in place and that these are maintained to the original high level.

“If the changes to standards and procedures required by PCI and integrated into quality standards are adopted for the operation of the complete business,” Edwards said, “[then] the compliance requirements are met, and you have secure processes in place that are regulated and audited on a regular basis by an external source. Essentially, you are killing more than one bird with the PCI ‘stone’.

Advantages of PCI

In addition to the long-term business advantages that can be gained from implementing PCI, organisations can realise several first-mover advantages. The most obvious advantage of PCI is to secure the business

and avoid the various penalties that an unsecured business could suffer. Additionally, Baker said, “By moving early to PCI, businesses have time to plan properly and deliver compliance cost-effectively.”

“There is increasing pressure on all organisations to be able to demonstrate corporate social responsibility, and PCI certainly is a significant step in this direction,” Wilson said.

PCI compliance can also be a business ‘good news story’, with advantages to be gained from developing positive PR messages about it. “There is increasing pressure on all organisations to be able to demonstrate corporate social responsibility, and PCI certainly is a significant step in this direction,” Wilson said.

Furthermore, there is opportunity to negotiate better commercial terms for the implementation and auditing of the systems while the implementation of PCI requirements is new to the market

And, in the longer term, customers will typically seek out merchants they consider are ‘safe’. In time, they will become confident and loyal customers who come back again and pass on their recommendations to others.

With fraud and data security featured regularly in the media headlines, a strong data security policy is essential to give an organisation a competitive edge, increase its revenue and improve its bottom line. With the countdown towards PCI compliance beginning, there is everything to play for. Organisations can harness some great opportunities that could positively affect their business performance and their relationship with customers. The penalties for noncompliance are immense; however, the rewards for achieving compliance and improving business processes could be the difference between business growth and stagnation. Organisations know what they have to do and are creating the systems of the future.

Profiting from PCI

About ACI Worldwide

Every second of every day, nearly 800 customers around the world rely on ACI solutions to process payments, manage risk, automate back-office systems and provide application infrastructure services. More customers use ACI software to manage higher payment volumes, of greater diversity, across more platforms and geographies than any other provider in our field. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.

What Payment Application Best Practices (PABP) Validation Means to ACI

ACI Worldwide and our customers experience several benefits when our products undergo a PCI and Payment Applications Best Practices (PABP) security assessment.

Market Leadership

Application and transaction security have always been a critical part of ACI's product design strategy. ACI's PABP security assessment program is an effort to be proactive, rather than reactive, in addressing today's evolving security standards. The posting of ACI applications on Visa's 'validated payment applications' Web page demonstrates our commitment to security.

Customer Expectations

Our customers frequently ask whether ACI products are CISP-compliant. They are, and the Visa validation lends credibility to our claims that ACI products are compliant.

Industry Trends

ACI's assessment program allows ACI products to address several industry trends and mitigate the risks to our customers.

Cybercrime is thriving. Massive data theft due to open systems and the Internet, the ease of selling stolen identities and card information, and ineffective law enforcement across international boundaries creates a breeding ground for organised fraud rings. Financial institutions must diligently implement strong corporate security policies.

Legislative pressures are increasing. Corporate accounting scandals, consumer privacy, identity theft and credit card fraud are evoking state and federal legislation requiring heightened security standards.

PCI mandates and enforcement are increasing, and adoption of PCI Standards is greater than ever. We are also aware that at least one large global payment processor requires that all of its application vendors are PCI validated.

These industry trends amplify the value of ACI's commitment to security and its security assessment program.

Customer Compliance

ACI provides PCI-compliant products and best practices guidance before our customers embark on their compliance initiatives. With the PABP validated status, customer application audits can be simplified, which in turn reduces the customer's total cost of compliance.

Liability

Several recent lawsuits and legislative initiatives address damages due to security breaches. In recent cases, damages have been assessed for costs of reissuing cards, brand damage and forensic expenses. Compliance with PCI Standards not only provides physical and logical protection against compromise, but also provides a level of protection from liability.

ACI Worldwide's Security Assessment Program

Since 2005, ACI has engaged Solutionary, a Visa accredited security assessor, to review strategic products using Visa's CISP PABP assessment program. Currently, three ACI products have been validated by Visa CISP: BASE24-atm[®], BASE24-pos[®], and the ACI Retail Commerce Server[™]. Most of ACI's other products are in various stages of remediation or reassessment. A continuous stream of validations is anticipated over the next year to provide a complete assessment of all products.

All product names are trademarks or registered trademarks of their respective companies.