Every organization that accepts payment cards is well aware of the challenges surrounding Payment Card Industry Data Security Standard (PCI DSS) compliance. The standards continue to evolve, as does the technology that is available to help address requirements. New threats to cardholder data are continually appearing, crafted by increasingly sophisticated hackers that are often part of organized crime rings. As long as you accept payment cards, PCI DSS requirements are here to stay.

First, the security standards represent industry best practices derived from a combination of preventative, detective and responsive controls that should be applied to processes, people and technologies across an organization. However, it's important to note that PCI DSS compliance is not a one-time event; it is an active, ongoing effort that involves constant monitoring and optimizing as threats and attacks evolve. It involves the management of risk associated with all card data, including:

- Who has access to data that is processed, transmitted, and/or stored
- Card skimming or tampering at the swipe terminal
- Supplier and employee conduct
That’s why, at the heart of PCI DSS compliance lies in both business security and risk management. Instead of focusing on compliance – especially setting security controls and adopting a particular technology to comply with a specific regulation or mandate – organizations should take a broader view and address their underlying business information security. Doing so enables them to conform to the various requirements through a single discipline: information security management.

This paper examines some best practices around addressing PCI DSS compliance – including the aforementioned security and risk management view, and provides information on many of the technologies that are available today that can help your business not only become compliant, but help maintain compliance long-term.

WHO IS LIABLE?

Any organization that accepts card payments is required to be compliant with PCI DSS. The only way to eliminate your PCI DSS scope is to stop accepting payment cards. The consequences of non-compliance range from penalties that can soar to $400,000 per year for the larger Level 1 and 2 merchants, to loss of consumer confidence that can irreparably damage – or bankrupt – the business itself. Headlines announcing the latest data breach appear almost weekly. The United States has continued to see the highest amount of credit card fraud in the world, accounting for 47 percent of all global fraud.² Most concerning, perhaps, is the continuing onslaught of new methods of attack, such as mobile malware.

PCI DSS BACKGROUND

While maintaining compliance can be costly, both from a technology and annual compliance assessment standpoint, the standards – maintained by the PCI Security Standards Council – can actually be beneficial to your overall business. Because PCI DSS is based on the international standards for information security programs, specifically ISO 20001, PCI DSS compliance can provide a framework to support other common regulatory standards, including the Health Insurance Portability and Accountability Act (HIPAA/HITEC) in healthcare and Sarbanes Oxley in finance. (However, since PCI DSS strictly addresses the protection of payment card data, businesses should not use PCI DSS as the only tool to address other regulatory requirements).

WHAT IS THE PCI SECURITY STANDARDS COUNCIL?

Formed in 2006 by Visa®, MasterCard®, American Express®, Discover® and JCB® to enhance payment account data security, the council manages the PCI Security Standards governing:

- Anyone who stores, processes or transmits cardholder data
- Payment application software development
- Payment hardware manufacturing

The council also trains and accredits:

- **Internal Security Assessors (ISAs) and Qualified Security Assessors (QSAs)** – Companies that can conduct PCI DSS validations
- **Approved Scanning Vendors (ASVs)** – Companies performing network vulnerability scan
- **PCI Forensic Investigators (PFIs)** – Companies performing forensic investigations

For more information, visit [pcisecuritystandards.org](http://pcisecuritystandards.org).
KEYS TO PCI DSS SUCCESS

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>PEOPLE</th>
<th>TECHNOLOGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationalize acceptance processes to reduce storage processing and transmission of card holder data</td>
<td>Provide on-going training for handling payment cards</td>
<td>PTS validated hardware terminals protect end points against tampering and skimming</td>
</tr>
<tr>
<td>Security policies and procedures that comply with PCI DSS</td>
<td>Implement organization wide security policy</td>
<td>PA-DSS validated applications ensure PCI grade security is built into the POS</td>
</tr>
<tr>
<td>Consistent processes and routines to protect card data and remain PCI DSS-compliant</td>
<td>Adopt best practice security procedures</td>
<td>P2P encryption and tokenization technologies further reduce scope and risk</td>
</tr>
</tbody>
</table>

APPROACHING RISK ACCEPTANCE

When taking a security and risk management approach to compliance, your organization should make informed decisions – about the risks that you can afford to accept, those that you can’t afford to accept and those that you are prohibited from accepting. An example of the latter is the practice of storing “track data” (data stored in the magnetic strip) or sensitive authentication data (i.e. card verification value, PIN, etc.), beyond the transaction authorization. Both practices are subject to immediate fines by the card brands.

Conversely, it is permissible to store card account data, as long as you comply with PCI DSS requirements to protect it. For this reason, it’s critical that your risk acceptance decisions not be managed in a vacuum. Security and technology teams need to collaborate closely with business decision makers to ensure that there is a valid driver for each business process impacting security and compliance. Armed with an understanding of business processes and the accompanying risks, you can take appropriate risk acceptance and management action to address exposures. After all, everyone has a stake in your organization’s survival and PCI DSS success.

FOCUS ON LONG-TERM SUCCESS

A common mistake organizations make is taking a reactive approach to compliance in general, including PCI DSS compliance, seeking a new “fix” for each new regulation. A better approach is to focus on information security risk management for the long term. Successful companies don’t just comply with the mandates as they are created, but instead build an information security program that provides a solid foundation across the organization to address mandates before they occur.

Again, it is the blending of people, processes and technology that makes the approach viable. Put information security and risk management in place correctly once, and you also successfully avoid repeatedly requiring cultural and behavioral changes in your organization that are difficult to enact and police. The initial process of incorporating information security into “business-as-usual” activities may involve a re-alignment on how you currently run the business. This could also require a commitment from all levels of the organization and is often a difficult “cultural change” to the business. Having security “baked in” to products or processes can enable you to focus your resources on your business and can help with the long-term sustainability of your PCI DSS compliance program.

Avoiding this thorough assessment is another common pitfall of the compliance strategy: focusing on a “fix” that simply does not make long-term sense. For example, if you are seeking an encryption solution because you are storing cardholder data, ask why you are storing the data at all, and if continuing to do so is still justifiable. The answer, we have often found, is a resounding no. There is usually not a true business need.

SOME QUESTIONS YOUR ORGANIZATION SHOULD ASK INCLUDE:

- What hardware and software do we have in place for payment acceptance?
- Are we using a third-party for payment processing, as opposed to a direct “acquirer”?
- Do our legacy cardholder data business processes make sense in light of:
  - Investments we will need to make
  - Processes we will have to implement
  - Effort we will have to exert
  - Discipline we will have to maintain

...To become and remain compliant?
KEY TECHNOLOGY AND PROVIDER CONSIDERATIONS

KNOW YOUR OPTIONS AND CHOOSE WISELY

No doubt you already have some data protection technologies in place, but if you are looking to adopt other security products, remember that whatever you purchase, it can’t make you PCI DSS-compliant. It may help reduce your PCI DSS scope, but no technology will ever eliminate your responsibility and liability if cardholder data is accessed by unauthorized parties. In short, when it comes to PCI DSS compliance, there is no silver bullet.

In addition, PCI DSS does not require you to purchase any specific product or technology to become compliant. That is strictly a decision to be made by your technology, security and line of business executives.

ASSESS YOUR ENVIRONMENT

As you examine your technology options, keep in mind any issues you may have around:

- Its implementation
- Whether the technology addresses any or all compliance requirements
- Whether the technology will contribute to more problems
- Whether you are operationally positioned to get maximum benefit out of your investment

Your goal should always be to implement the technologies that can help your business become compliant sooner and stay in compliance longer.

Third-party service providers are often enlisted to provide payment acceptance technologies and solutions. This can be a viable strategy to not only address PCI DSS, but also to reduce the costs of compliance, especially for organizations that lack the expertise or resources to effectively manage the technology.

Since the liability for card data protection rests with your business, be very certain that you understand what the third party is – and is not – managing for your PCI DSS compliance effort. If the service provider is not PCI DSS-compliant, it can place your organization at an elevated risk if they experience a data breach. Visa and MasterCard maintain a list of registered PCI DSS-compliant providers.

Consider the Ramifications of a Data Breach

From a payment acceptance perspective, you are still liable for the cardholder data loss even if you have outsourced processing to a third party. You should review your agreement with the service provider to ensure there are provisions you can take to help protect your business in the event of a data breach. Consider this: if your service provider is compromised, other companies using that provider will likely be affected as well. If the service provider is not strong financially, it may not survive the incident to compensate your loss.

Always review your third-party agreement with your legal representative to ensure that you understand the full agreement.
**COMMON COMPLIANCE-ENABLING TECHNOLOGIES**

**Account Number Masking** is primarily a display technology that "masks," or obscures, the full personal account number (PAN), showing only partial numbers. While the underlying data is still stored in your system, the displayed number is suppressed on a need-to-know basis, so it is useful in limiting PCI DSS scope by denying end-users access to the full PAN. Masking is neither tokenization nor data encryption, and it does not employ hashing or encryption algorithms. Unlike account number masking, account number truncation contains only the first six and four digits of the card account number.

**Virtual Terminals** provide remotely hosted payment acceptance on a web page that you connect to using a Secure Sockets Layer (SSL)-encrypted link. From there, you can enter payment card data. While virtual terminals support ecommerce or mobile transactions, they can also operate in conjunction with a card reader to support card-present transactions, and can incorporate tokenization. Virtual terminals are also ideal for call center and customer self-service business models.

**ORBITAL® VIRTUAL TERMINAL** enables you to securely process and manage payments accepted online, by phone or mail. It eliminates the need for additional terminal hardware, software updates, dedicated phone lines and related maintenance. You can use it to initiate card authorizations, settlements, refunds and other activity, with options to automatically or manual settle transactions. Available to at no additional charge to Orbital Payment Gateway users, Virtual Terminal requires you to have computer, a web browser, Internet access and a Chase Paymentech merchant account.

**Tokenization** replaces the primary account number (PAN) with a value, or "token" that can’t be reversed and traced back to the actual account number after the transaction is authorized. A tokenization server creates the tokens, tracks the relationship of tokens to PANS, and translates tokens back into PANs. This technology supports PCI DSS compliance by enabling you to avoid storing cardholder data (since you are storing tokens instead), and it reduces your risk in the event of a compromise. However, tokenization does not address the security gap at the point of acceptance, where the cardholder data is initially gathered to be converted into a token.

**SAFETECH® TOKENIZATION** helps you ensure that if cardholder data is breached, the information is of little use to a hacker, since Chase Paymentech manages the decryption key. You can use Safetech Tokenization in conjunction with Safetech Page Encryption (see below) to protect data in transit and at rest, two factors that affect your PCI DSS scope.

**Page Integrated Encryption** involves outsourced ecommerce payment acceptance and processing that helps you ensure that cardholder data does not reside in your ecommerce environment, helping you reduce your PCI DSS scope. It encrypts the cardholder data at the consumer’s browser page, with both the decryption and the payment processing performed by a third party. Even with page integrated encryption, you must still take measures to protect your ecommerce security to prevent session hijacking and redirect attacks.

With **SAFETECH PAGE ENCRYPTION**, Chase Paymentech manages the process described above. Although not required, we strongly recommend that you use both Safetech Page Encryption and Safetech Tokenization to protect cardholder data and reduce your PCI DSS scope.
Point-to-point encryption (P2PE) is a point-of-sale (POS) terminal technology that encrypts card data at the time of the swipe and decrypts the data outside of your environment. The P2PE technology provider manages the decryption key, helping you reduce your PCI DSS scope. Once encrypted, the card data is not tokenized; it remains the value of the PAN. Implementation requires PCI DSS-validated P2PE hardware.

SAFETECH ENCRIPTION encrypts cardholder data for card-present transactions, including tapped, contactless, dipped, swiped and manually keyed. It is designed to integrate with most POS systems. Since we manage the decryption key for you, you can potentially reduce your risk if a system breach occurs.

CHASE MOBILE CHECKOUT provides P2PE for mobile payments. To use this solution, all you need is a mobile device with the Chase Mobile Checkout app, our card reader and a Chase Paymentech merchant account. You can use it to accept payments on all major credit cards and signature debit cards, with the assurance of knowing cardholder data is encrypted as soon as the card swipe occurs.

A hosted pay page provides outsourced ecommerce payment acceptance and processing, keeping cardholder data out of your ecommerce environment, and enabling you to avoid receiving or transmitting cardholder data, potentially reducing your PCI DSS scope. As with other security technologies, you must maintain additional measures to protect your Internet security.

ORBITAL HOSTED PAY PAGE directs customers to a secure server to enter payment details onto a Chase Paymentech form at the time of checkout. You receive notification from Chase Paymentech when the transaction is approved. You can use Hosted Pay Page in conjunction with the Orbital Customer Profile Management Service to replace the card data with a token that represents the transaction or customer.

HOW DOES PCI DSS RELATE TO EMV?

EMV, which stands for Europay, MasterCard® and Visa® uses a chip, or microprocessor, that's embedded in a card to make payments at the POS. The chip uses encryption to protect, secure and store sensitive authentication data within it, and validates the card during each interaction with the EMV-enabled POS terminal. EMV does not support or replace PCI DSS compliance, because the clear card data is still being transmitted once it leaves the EMV terminal. However, EMV has been shown to significantly reduce counterfeit card fraud. But in markets where EMV has been rolled out, studies showed sometimes dramatic shifts in fraud to less secure environments, specifically card-not-present (CNP). In preparing for the EMV rollout in the United States – generally considered to be October 2015 due to a fraud liability shift enacted by the card brands at this time – you should consider adopting solutions that will enable your organization to reduce CNP fraud, such as 3D Secure and Safetech Fraud Tools.

APPROACH PCI DSS COMPLIANCE HOLISTICALLY

Regardless of the technology solutions you implement or providers you choose to work with to support PCI DSS compliance, it's imperative to approach it as a long-term strategy that takes into account the needs of the business as well as current and future technology needs and challenges before selecting any technology or provider. The best forward-thinking approach involves a focus on security, rather than “getting compliant,” with an eye toward eliminating obsolete practices or processes that may not only inhibit compliance but also no longer support your organization's business needs. Remember that regardless of the technology and controls you put in place, PCI DSS responsibility remains with you, the merchant. Chase Paymentech can provide you with both the expertise and resources to help you become compliant quickly – and stay in compliance.
Why Chase Paymentech

With nearly 30 years of payment processing experience, Chase Paymentech offers an array of services to support your PCI DSS compliance needs, including proactive outreach to your business regarding changes in card brand rules, security alerts, new fraud trends or a potential compromise – often before you have detected the issue. We provide:

**Annual training** – If you have an assigned Chase Paymentech account representative, we offer annual PCI DSS training sessions so your technical implemeniter and auditor can discuss questions and concerns with representatives from the PCI Security Standards Council, the payment brands, and other industry experts.

**Advocacy and dispute resolution** – We can facilitate direct conversations with the payment brands.

**Faster detection and response** – Our unique position facilitates information flow to your organization, for both fraud and PCI DSS compliance-related insight.

**Teams dedicated to compliance**

- Chase Paymentech's Compromise Investigations Team provides information, leadership, and support when cardholder data compromises occur, and a focus on helping you minimize losses.
- Our Merchant Compliance Team supports adoption of cardholder data security compliance programs by all of our merchants, their service providers and payment application providers in the United States, Canada and Western Europe.
- Our Product Management Team provides information on – and support for – technology solutions that can help you protect cardholder data.

MAKE THE RIGHT CALL

For more information about PCI DSS compliance and compliance-enabling technologies, contact your Chase Paymentech representative, or visit us at chasepaymentech.com.