Securing Payment Card Data in Flight

How to protect your sensitive payment data in customer-present and call center environments

CyberSource®

CyberSource is a Visa solution VISA

Delivering a Trouble-Free Customer Experience

Delivering a Trouble-Free Customer Experience

Securing Card Data with P2PE

Differentiating Between Listed and Unlisted P2PE Solutions

Simplifying Compliance with a Listed P2PE Solution

Reducing Your Risk Profile, Maximizing Your Return

For More Information

Data breaches are on the rise for merchants of all sizes. Hackers succeed in many of these cases by gaining access to point-of-sale (POS) systems through a variety of methods. They use phishing, exploit compromised account credentials, and attack operating system vulnerabilities on the POS system or attached auxiliary systems. Once they gain access, they secretly install malware that extracts the data they want to steal.

What can your business do to deliver a trouble-free customer experience and prevent the significant damage that can be caused by breaches?

High Cost of Data Breaches

Recent studies of retail data breaches have attempted to estimate the average cost of a data breach, with the following results:

- **$172** average cost per record[1]
- Volume-specific average costs, ranging from **$67,480** for 1,000 records[2] to **$8.8 million** for 100 million records[3]

EMV technology helps mitigate POS risk, but it cannot protect payment data from hackers. By verifying the authenticity of cards, EMV makes creating counterfeit credit cards more difficult for fraudsters. Still, EMV technology leaves credit card account numbers, expiration dates, and cardholder names vulnerable. You need another technology to protect that data.

Point-to-Point Encryption (P2PE) is an effective supplement to EMV and other technologies. It helps safeguard data at the point of acceptance and in transit, while enabling you to control costs.

[1] Ponemon 2016 Cost of Data Breach Study. Cited in Coalfire, "Impact of PCI P2PE," prepared for Bluefin Payment Systems, 2017.
[2] Verizon 2015 Data Breach Investigations Report (DBIR). Cited in Coalfire, "Impact of PCI P2PE," prepared for Bluefin Payment Systems, 2017.
[3] Ibid.

Securing Card Data with P2PE

Delivering a Trouble-Free Customer Experience

Securing Card Data with P2PE

Differentiating Between Listed and Unlisted P2PE Solutions

Simplifying Compliance with a Listed P2PE Solution

Reducing Your Risk Profile, Maximizing Your Return

For More Information

P2PE has emerged as a powerful and effective way to protect POS and call-center environments from threats to in-flight data. The term P2PE is used by the PCI Security Standards Council (SSC) to refer to its terminal-based encryption standard. This standard is designed to help ensure account data can be transferred through the merchant environment safely.

A P2PE solution encrypts payment data at the data entry point on the POS terminal, and then transmits the encrypted data securely for payment processing. The encryption continues to safeguard the card data as it moves from your network to a decryption and processing gateway. By using strong encryption together with sound practices for key management and device management, P2PE effectively addresses the risk of compromising customer card data in transit.

To meet the standard set by the PCI SSC, a P2PE solution or service must meet three high-level requirements:

- The card data must be encrypted using strong cryptography.
- The encryption must be performed within a PCI P2PE-approved hardware device.
- Decrypting the data must not be possible within the merchant environment.

Solutions and services that meet these requirements can effectively secure cardholder data in flight within your software, systems, and network.

Differentiating Between Listed and Unlisted P2PE Solutions

Delivering a Trouble-Free Customer Experience

Securing Card Data with P2PE

Differentiating Between Listed and Unlisted P2PE Solutions

Simplifying Compliance with a Listed P2PE Solution

Reducing Your Risk Profile, Maximizing Your Return

For More Information

To help ensure P2PE solutions deliver the protection that vendors promise, the PCI SSC standard for P2PE established specific controls that vendors must implement to have their product considered an approved P2PE solution or component. Each control is associated with identified, real-world threats that can jeopardize the security of your customers' credit card data. That means it is essential to ensure any P2PE solution or service you select complies with these controls.

"Listed" solutions have been validated as meeting the PCI P2PE standards. Solutions that have not been validated, but still provide functions such as encrypting within the POS terminal and decrypting outside the merchant environment, are generally called "unlisted" P2PE solutions, or end-to-end encryption (E2EE).

There are several disadvantages to unlisted solutions. For example:

- There may not be a way for you to know whether the solution provider has fully addressed the controls identified by PCI SSC as necessary to properly protect account data.
- As a result, you will need to perform a thorough compliance assessment using the authorized self-assessment questionnaire (SAQ) D.
- You might consequently need to implement additional security measures to bring the solution up to standard—which can be costly and time-consuming.

Listed P2PE solutions, on the other hand, eliminate the uncertainty of unlisted solutions. With a listed solution, you can be confident it meets the criteria for the PCI P2PE program. You have the assurance that even if your data is captured, malware will not be able to read it.

Simplifying Compliance with a Listed P2PE Solution

Delivering a Trouble-Free Customer Experience

Securing Card Data with P2PE

Differentiating Between Listed and Unlisted P2PE Solutions

Simplifying Compliance with a Listed P2PE Solution

Reducing Your Risk Profile, Maximizing Your Return

For More Information

A P2PE solution can not only protect your data and your brand, but also save you time and effort. By using a listed solution—one validated as meeting the P2PE standard—you can substantially reduce your PCI compliance requirements.

It only makes sense: since merchant systems can no longer access data that is properly encrypted, a listed P2PE solution effectively reduces the number of networks and systems considered to be within the scope of the PCI assessment. With proper implementation of a listed solution, you might be eligible for the authorized self-assessment questionnaire (SAQ) for P2PE and answer 90 percent fewer questions than if you were using SAQ D.

CyberSource clients now have access to these benefits with a PCI-validated P2PE solution (see sidebar). This Bluefin-powered encryption solution is designed to help protect data across all segments of your network, including wireless connections and processing servers.

P2PE from CyberSource

Safeguard data generated through in-person payments as well as payments handled by your call center agents with CyberSource Point-to-Point Encryption, powered by Bluefin.

- **Reduce vulnerabilities:** Reduce risks by helping to prevent unencrypted transaction data from touching your systems.
- **Avoid POS malware threats:** Help prevent POS malware residing on your system from capturing any readable card data by maintaining data in an encrypted state.
- **Decrease PCI scope:** Lessen the scope of PCI compliance by keeping unencrypted data out of your environment.

Reducing Your Risk Profile, Maximizing Your Return

Delivering a Trouble-Free Customer Experience

Securing Card Data with P2PE

Differentiating Between Listed and Unlisted P2PE Solutions

Simplifying Compliance with a Listed P2PE Solution

Reducing Your Risk Profile, Maximizing Your Return

For More Information

Stolen credit card account data is very costly—to the consumer, the card networks, and you, the compromised merchant. These costs can include fines, penalties, consumer notification and credit monitoring for those affected, forensic investigation, remediation, loss of business, damage to relationships, and damage to consumer reputation and trust.

In today's credit card transaction environment, P2PE is a necessary technology to protect card data in transit and is part of a holistic payment security approach that also includes EMV. With P2PE, you can add another layer of protection to your customers' information and decrease your risk profile while reducing costs.

The benefits of a listed P2PE solution include reduced PCI compliance scope and state-of-the-art security. You can also realize a very positive return on your P2PE investment (see sidebar).

Control Costs and Increase ROI with P2PE

A recent independent study by Coalfire for Bluefin Payment Systems shows the total cost of ownership (TCO) and return on investment (ROI) for a P2PE solution and the resulting PCI compliance scope reduction.

- **TCO: Less than 2/3** that of the current state without a P2PE solution[4]
- **ROI: 15x return** over the life of the solution[5]

Costs used in these calculations are based on illustrative examples, and results may vary according to the ways in which a business may model its own compliance costs.

[4] Coalfire, "Impact of PCI P2PE," prepared for Bluefin Payment Systems, 2017.
[5] Ibid.

For More Information

To learn more about PCI P2PE and how it can benefit your organization, visit: www.cybersource.com

Portions of this document are drawn with permission from the Coalfire Systems study, "Impact of PCI P2PE," prepared for Bluefin Payment Systems, 2017.

CyberSource, a wholly owned subsidiary of Visa Inc., is the only integrated payment management platform built on secure Visa infrastructure, with the payment reach and fraud insights of a massive $384 billion global processing network. CyberSource and Authorize.Net payment management solutions help businesses grow sales, mitigate risk, and operate with greater agility.

CyberSource®

CyberSource is a Visa solution VISA