



## DATA INTERCEPT SOLUTIONS

**SOLUTIONS:** Data Intercept Solutions Paymetric's **Data Intercept Solutions** keep sensitive cardholder data from entering merchants' payment processing systems, dramatically reducing the cost and effort required for merchants to become fully compliant and secure.

### THE PROBLEM

Any merchant that handles, processes or stores sensitive cardholder data is required to comply with the Payment Card Industry Data Security Standard (PCI DSS). Achieving compliance with the 12 PCI DSS requirements has proven to be onerous and costly for most merchants. And with data breaches continuing to increase, and the cost of such incidents rising, merchants who store cardholder data on-site are particularly vulnerable – even if that data is protected with encryption. That is why it is becoming increasingly popular for merchants to seek out ways to eliminate their liability to protect stored cardholder data and reduce or even eliminate PCI audit scope.

The total cost of a data breach grew to \$204 per record in 2009.<sup>1</sup>

### THE ANSWER

**Data Intercept Solutions** is a technology developed on a simple premise – capture card numbers as early in the work flow as possible. The solution leverages Paymetric's award-winning XiSecure On-Demand tokenization technology and ensures that cardholder data never enters enterprise payment acceptance systems – SAP,<sup>®</sup> ERP, CRM, legacy applications and Web stores. Merchants no longer store cardholder data on-site, but instead, store tokens – eliminating the liability to protect that sensitive information and the associated cost and risk of doing so.

If properly architected, Paymetric's **Data Intercept Solutions** may help merchants reduce PCI audit requirements from 205 to as low as 14, allowing significant savings.<sup>2</sup>

How does it work? Sensitive information is intercepted and tokenized at the time of entry. This secure token is then provided to the merchant for use in authorization and settlement. A "token" is a surrogate value that represents the real number, but is useless to thieves, and can be used just like the real card number to support on-going customer interactions like recurring payments. Raw data never enters the merchant system. **Data Intercept Solutions** offer the ultimate breach protection, and merchants can drastically reduce the scope of their PCI audit by eliminating transmission and storage of sensitive cardholder data.

 **paymetric**

TRUSTED SOLUTIONS. SECURELY INTEGRATED.

# SOLUTIONS Data Intercept Solutions

## FEATURES

- Prevents sensitive cardholder data from entering merchants' enterprise payment acceptance systems
- Substitutes credit card numbers with "tokens," rendering the data useless to thieves
- Provides logging information for PCI audit purposes

## BENEFITS

- Easily distributable across an environment with multiple work stations
- Eliminates fees, fines and legal costs associated with a data breach
- Reduces scope and cost of achieving and maintaining PCI compliance
- May qualify merchants for Self Assessment Questionnaire A (SAQ-A), reducing the number of compliance requirements from 205 to 14

## DATA INTERCEPT FOR ECOMMERCE

When paying for products or services in the merchant's Web store, sensitive cardholder data is transparently intercepted by Paymetric from your client's web browser. Paymetric generates a token for the intercepted number and returns it to the merchant's web server to be routed for authorization and settlement. The process, which takes seconds to complete, is entirely transparent to the customer. The merchant never transmits, processes or stores the RAW cardholder data, but instead handles only the token which can be used for day-to-day activity.

## DATA INTERCEPT STANDALONE

When taking orders, merchants access the **Data Intercept Solutions** via a Paymetric web browser designed to instantly generate a token that can be entered into enterprise payment acceptance systems such as SAP, ERP, legacy applications or POS for authorization and settlement. The merchant never transmits, processes or stores the RAW cardholder data, but instead handles only the token which can be used for day-to-day activity.

## DATA INTERCEPT FOR SAP

Card numbers are entered into a special field that automatically pops up when a customer service rep attempts to enter them into the payment card field located in the SAP order entry screen. The number is then routed to Paymetric's secure data vault for tokenization. The token is returned to SAP and automatically populates the original payment card field to be used for authorization and settlement. Because the real number was intercepted using SecureEntry™ technology powered by PrimeSys, it never enters the SAP system, placing it in a position to be removed from PCI scope.

Paymetric, Inc. / 11175 Cicero Drive, Suite 175  
Alpharetta, Georgia 30022 / tel 678-242-5281  
fax 866-224-5867 / [www.paymetric.com](http://www.paymetric.com)

© 2011 Paymetric, Inc. All rights reserved. The names of third parties and their products referred to herein may be trademarks or registered trademarks of such third parties. All information provided herein is provided "AS-IS" without any warranty. <sup>1</sup>2009 Annual Study: cost of a Data Breach, Ponemon Institute. <sup>2</sup>Please consult your acquirer or QSA to confirm that Paymetric's Data Intercept solution will qualify you for PCI SAQ-A.) 04-2011/PM11\_009



TRUSTED SOLUTIONS. SECURELY INTEGRATED.

