



VALUE-ADDED SOLUTIONS: DATA INTERCEPT

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

THE PROBLEM

In today's market, it's expected for a merchant to accept electronic payments. And so merchants have invested in costly systems, shouldering the risk and expense of handling, processing and storing cardholder data. Yet merchants face tremendous pressure to further secure this sensitive information. With data breaches on the rise, the Payment Card Industry Security Standards Council (PCI SSC) has tightened compliance requirements. So as a result, merchants feel forced to invest even more in costly solutions that may still leave systems vulnerable.

The total cost of a data beach grew to \$202 per record compromised, an increase of 2.5% since 2007.¹

BENEFITS

- Prevents sensitive cardholder data from entering merchants' enterprise payment acceptance systems
- Substitutes credit card numbers with "tokens," rendering the data useless to thieves
- 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 14.²

THE ANSWER

Data Intercept Solutions for XiSecure On-Demand ensure that cardholder data never enters enterprise payment acceptance systems - SAP, ERP, CRM, legacy applications and web stores. How does it work? Sensitive information is intercepted and "tokenized" at the time of sale. This secure token then routes to the merchant for authorization and settlement. RAW data never enters the merchant system. **Data Intercept Solutions** offer the ultimate breach protection, while dramatically reducing the cost and effort to achieve PCI compliance.

With Paymetric's **Data Intercept Solutions**, merchants may be able to reduce PCI audit requirements from 205 to as low as 14, allowing significant savings.²

VALUE-ADDED SOLUTIONS: DATA INTERCEPT

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 solution 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.

SECURE ENTERPRISE PAYMENT ACCEPTANCE SOLUTIONS



Paymetric, Inc. / 19500 SH 249, Suite 300 / Houston, Texas 77070 / tel 713-895-2000 / fax 713-895-2001 / www.paymetric.com

Copyright 2009 Paymetric, Inc. All rights reserved. Paymetric and Paymetric Solutions are either registered trademarks, service marks, or trademarks of Paymetric, Inc. in the United States and/or other countries. Other trademarks appearing on this document are the property of their respective owners. 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. '2008 Annual Study: cost of a Data Breach, Ponemon Institute. 'Please consult your acquirer or QSA to confirm that Paymetric's Data Intercept solution will qualify you for PCI SAQ-A.) 08-2009/PM010