



# XISECURE ON-DEMAND FOR SENSITIVE DATA

## SOLUTIONS: XiSecure On-Demand For Sensitive Data

Protect sensitive data with tokenization technology to minimize risk and address legislative and compliance requirements.

### THE PROBLEM

As data security breaches and their associated costs continue to grow, industry regulations become more stringent and data breach notification laws come into effect, organizations are increasingly pressured to protect personally identifiable information (PII).

PII is information that can be used uniquely or with other sources to identify, contact or locate a single person. Examples of PII are: full name, email, social security number, IP address, license plate number, driver's license number, credit card numbers, medical records and HR records.

### THE ANSWER

**XiSecure On-Demand for Sensitive Data**, Paymetric's tokenization solution, affords businesses the opportunity to eliminate the storage and/or transmission of PII in enterprise systems and applications. By utilizing tokenization technology, companies can reduce the risk of a data security breach, and take advantage of the safe harbor that most breach notification laws provide to companies that secure PII. Because the solution is delivered on-demand, it is extremely affordable when compared to the investment businesses would have to make in costly encryption solutions. And your customers and employees can sleep better at night knowing their sensitive information is secure.

### THE EVOLUTION OF TOKENIZATION – FROM CARDHOLDER DATA TO PII

Tokenization was originally developed as a way for organizations to address the Payment Card Industry Data Security Standard (PCI DSS). As part of the standard, any merchant that processes, stores or transmits cardholder data is required to protect that data. Many organizations turned to encryption, a solution that proved costly and still left systems and applications vulnerable to attack. Enter stage right: tokenization.

Tokenization quickly became favored by merchants to protect stored cardholder data because it was a cost-effective solution that drastically reduced their risk and liability. Security analysts and even members of card associations like Visa have further endorsed the utilization of tokenization and have correlated the adoption of the technology with "best-in-class" results.

As data breaches continued to rise, other industry regulations (like the HITECH Act for the healthcare industry) soon followed the recommendations of the PCI DSS and mandated the protection of PII. Even federal and state governments have begun requiring public disclosure of breaches if reasonable measures to protect PII have not been taken.

Because tokenization is such a flexible technology, it can be easily adapted to protect any type of PII in any enterprise system or application. Paymetric's tokenization solution is proven and has been used to secure billions of transactions for top Fortune 100, 500 and 1000 clients around the globe.



TRUSTED SOLUTIONS. SECURELY INTEGRATED.

# SOLUTIONS XiSecure On-Demand For Sensitive Data

## ■ HERE'S HOW IT WORKS

Tokenization works by intercepting PII entered into enterprise systems or applications and replacing it with a surrogate value known as a "token." A "token" is a unique ID created to reference the actual data associated with the encrypted data. The original data is stored off-site in Paymetric's secure data vault.

## ■ BENEFITS

### FORMAT PRESERVING TOKENS

FlexTokens powered by XiSecure On-Demand, Paymetric's format preserving tokenization solution, brings organizations the desired adaptability to protect multiple types of sensitive information. FlexTokens maintain the original length and format of the data so that organizations can leverage tokenization technology to protect any type of sensitive information that resides within their enterprise. Now businesses can roll-out a tokenization strategy for their entire organization with minimal impact to their existing IT infrastructure.

### PROTECT PII AFFORDABLY

With an on-demand model there is no need to make large capital investments in costly encryption solutions. Instead, you can take advantage of a subscription based, affordable tokenization solution and an extra layer of security.

### ACHIEVE SAFE HARBOR FROM DATA BREACH NOTIFICATION LAWS

Many data breach notification laws will provide safe harbor to those companies that had taken some measure to protect the stolen data. By utilizing tokenization, your company would not have to publically disclose a breach, protecting your image and reducing the risk of increased attrition.

### INCREASE SECURITY AND PROTECT YOUR BRAND

With Paymetric's tokenization solution, **XiSecure On-Demand for Sensitive Data**, PII is never stored intact anywhere, eliminating accidental exposure and making it completely impossible for hackers to reassemble it through decryption or reverse engineering. This increased security allows companies to preserve their brand without the worry of unexpected fees, fines or legal costs associated with a data breach. The average cost of a data breach in the United States is \$6.65 million.<sup>1</sup> That equals \$204 per compromised customer record.<sup>1</sup>

### WITH TOKENIZATION IT'S BUSINESS AS USUAL

"Tokens" can be used in place of sensitive data throughout the enterprise to meet the demands of on-going customer and employee interactions and because they act just like the original data, there is no disruption to day-to-day operations.

Tokens are multi-use, meaning that the token has a 1:1 relationship with the original data. The same token returned from the initial entry of a social security number, for example, would then be returned for any subsequent entry of the same social security number. This supports source application functionality related to reporting, metrics, customer or employee queries and even fraud and loss prevention functionality.

## ■ STANDARD FEATURES

- Removes stored data from enterprise application databases
- Replaces PII in enterprise applications with tokens
- Stores tokens in an off-site, centralized and secure data vault
- Provides key management processes outside of enterprise applications, thus eliminating system and application down time

- Provides key rotation capabilities outside of enterprise applications
- Provides access logging for decryption requests
- Provides monitoring of decryption requests
- High Availability – 24x7 operation is supported via high availability mechanisms such as load balancing and database clustering
- Integrated back-up
- Disaster Recovery – A disaster recovery site provides recovery from total-site outages

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>Aberdeen Group – Avoiding a Kick to the Head, The Value of Tokenization for Protecting Stored Cardholder Data, 2010.  
<sup>2</sup>The Ponemon Institute: Cost of a Data Breach Study 2009.  
04-2011/PM11\_021

 **paymetric**

TRUSTED SOLUTIONS. SECURELY INTEGRATED.