



# Containing—and Reducing—the Burden of the Payment Card Industry Data Security Standard

## How the Cardholder Data Environment Impacts PCI DSS

---

According to VeriSign, the leading reason why businesses fail their PCI assessment is the failure to protect stored cardholder data.<sup>1</sup> It's possible for cardholder data to be used extensively throughout a business.

The challenge to secure cardholder data continues to compound as it is used in many places within businesses including:

- Transaction authentication
- Settlements
- Reconciliation
- Chargebacks
- Loyalty rewards programs
- Marketing
- Sales auditing
- Loss prevention

## Defining the Cardholder Data Environment

Every computer system and filing cabinet, along with every application that uses or stores sensitive card data is part of the overall cardholder data environment (CDE). As cardholder data is used beyond the point-of-sale (POS) and for purposes beyond transaction authentication, the CDE grows and likewise PCI DSS compliance and validation increasingly becomes more complex and costly. When business owners conduct their initial appraisal they learn about the extent of their CDE.



## **It's Possible to Limit—Even Shrink—CDE**

Every business that accepts payments cards has a CDE that comes under the purview of PCI DSS. It's possible to limit—and even shrink—the scope of the CDE to reduce or minimize your PCI DSS compliance and validation burden.

### **3 Ways to Limit CDE and Reduce PCI Compliance Costs**

#### **1. Restrict the use of cardholder data to only those applications directly pertaining to payments**

These applications include: transaction authentication, daily settlements, chargebacks, add-ons for items such as gratuities or recurring payments

#### **2. Use a token to retrieve stored cardholder data**

Tokenization is when a credit card is used in a transaction and, once authorized, the cardholder data is sent to a centralized and highly secure server called a “vault.” Then random unique number is generated and returned to your system for use wherever the cardholder data would be used. Credit card data has been removed from various business applications and replaced with a token.

#### **3. Outsource the data vault to a third party.**

Removing the data vault from the CDE—and handing the responsibility (and liability) for it over to the third-party service provider—further shrinks the environment that is subject to PCI compliance

<sup>1</sup> VeriSign Global Security Consulting Services, *Lessons Learned: Top Reasons for PCI Audit Failure and How To Avoid Them*, 2007, p. 4.