Office of the Secretary of State
Washington State Archives

Records Management Advice
Updated: August 2015
(Originally Issued: December 2014)

Destroying Non-Archival Records:
Sensitive Cardholder Data Obtained During Payment Card Transactions

Purpose: Provide guidance to local government agencies on lawful destruction of sensitive payment card/holder data to minimize public and agency risk.

Any local government agency that **processes, stores, or transmits payment card data** is required by the card provider (Visa, MasterCard, American Express, etc.) to comply with certain security standards to prevent cardholder data theft. In 2006, the Payment Card Industry (PCI) Security Standards Council established its Data Security Standard (PCI DSS), and in 2010 the Revised Code of Washington incorporated the standard into chapter 19.255 RCW, *Personal Information – Notice of Security Breaches.*

Part of the security standard stipulates that certain **Sensitive Authentication Data** is *forbidden* to be stored once the payment card transaction has been completed. This includes data that is used to authenticate electronic transactions where the card is not physically present, such as the Card Verification Value (CVV) or Card Validation Code (CVC) found on the front or back of the card and/or encoded in its magnetic stripe.

The State Auditor's Office has clarified what must be maintained for audit purposes by local governments when ***receiving*** credit card payments. Local governments should only maintain the **transaction number** assigned by the credit card company or the third party credit card processing vendor, ***not the entire primary account/credit card number***. Local governments are encouraged to comply with PCI DSS standards, including the requirements to render any stored primary account number or credit card number unreadable.

In an effort to mitigate financial risk to customers and the public agencies that serve them, the Local Records Committee (LRC) has approved specific disposition authority for Sensitive Authentication Data AND primary account/credit card numbers (collectively referred to as "Sensitive Cardholder Data") by approving DAN GS2014-030, ***Financial Transactions - Sensitive Cardholder Data***, which is located in the Financial Management section of the *Local Government Common Records Retention Schedule* (*CORE).* The State Auditor's Office has confirmed that it does not require this Sensitive Cardholder Data to be retained for audit purposes.

Please note that only **Sensitive Authentication Data** *as defined in current* PCI DSS standards **and** the **primary account/credit card number** may be destroyed under GS2014-030. All other elements of the record that are **made or received** by the agency (such as transaction number, date, amount, etc.) need separate disposition authority because they are required for audit purposes and must be retained in accordance with the appropriate ***Financial Transactions*** series.

PLEASE NOTE: This is no way requires that the agency create a record (or portion of a record) that it otherwise does not make or receive.

Additional advice regarding the management of public records is available from Washington State Archives:

www.sos.wa.gov/archives
recordsmanagement@sos.wa.gov

Destroying Non-Archival Records: Sensitive Cardholder Data Obtained During Payment Card Transactions

Common Methods of Destroying Sensitive Cardholder Data:

Under WAC 434-640-020, destruction of confidential records must reduce them to an illegible or otherwise irretrievable condition.

For **existing database records**, Sensitive Cardholder Data (Sensitive Authentication Data **and** the primary account number/credit card number) should be deleted. This deletion should also be applied to any backups of these records.

Existing paper records at the agency should have any Sensitive Cardholder Data removed in some permanent fashion, such as physically cutting out the sensitive portion or covering it and then photocopying or scanning the record. Similarly, **records that have already been scanned to digital format** in accordance with the "scan and toss" requirements should have this data redacted from both the image and any metadata.

Existing emails containing Sensitive Cardholder Data should be redacted and resaved in electronic format, retaining as much of the original metadata as possible.

Point forward, both paper-based and electronic records should be created in a manner that ensures that all Sensitive Cardholder Data is retained separately or can be easily separated from the rest of the transaction record (e.g., as a separate data field, on a Post-It note attached to the transaction record, etc.) This approach should be documented in official agency procedures.