Office of the Secretary of State
Washington State Archives

Records Management Advice
Issued: December 2014

Destruction of Non-Archival Records:
Destruction of Sensitive Authentication Data Obtained During Payment Card Transactions

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

Any state or 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. 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 this information by approving DAN GS2014-030, ***Financial Transactions - Sensitive Authentication Data***, which is located in the Financial Management section of the *Local Government Common Records Retention Schedule* (*CORE) Version 3.1.* The State Auditor's Office has confirmed that it does not require this Sensitive Authentication Data to be retained for audit purposes.

This is the first time that the LRC has ever approved destruction of a ***portion*** of a record. However, given the enormity of the potential security risk, it was deemed necessary and appropriate. Please note that **only Sensitive Authentication Data as defined in the current PCI DSS may be destroyed** under GS2014-030. All other elements of the record (including **but not limited** to the primary account number, the credit card number *(if different),* and the transaction amount) are required for audit purposes and must be retained in accordance with the appropriate ***Financial Transactions*** series.

Common Methods of Destroying Sensitive Authentication 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 Authentication Data should be deleted. If a field in a batch of transaction records consists entirely of Sensitive Authentication Data, that field may be completely removed as soon as the transactions are complete. This deletion should also be applied to any backups of these records.

(continued next page)

Existing paper records at the agency should have any Sensitive Authentication 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 Authentication 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 Authentication 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.