

Recommended Best Practices

Electronic Deposit Services

Check Retention Archive Requirement

[State Archives 166-300-0025 \(15\)](#) requires the original paper check to be retained for a period of 30 days.

Secure Storage

It is recommended that customers use commercially reasonable methods to securely store all source documents and all related banking information until destruction. For example, many depositors use tamper proof poly bags to store items. It is recommended to have a documented notification process in the case of a data breach; or theft of physical checks that have been electronically deposited. [OST Data Security Policy 02.18.13](#)

Business Continuity Planning

State agencies utilizing RDC are required to have a business continuity plan in place that documents procedures for making physical deposits in the event of disaster or if systems are down and the agency is not able to deposit funds electronically. Agencies should have physical deposit slips on hand for each deposit account prior to going live with RDC. Deposit slips can be ordered by contacting [Cash Management Manual Section IV](#).

Secure Destruction

After the retention period, items need to be securely destroyed. Cross shredding is strongly recommended.

Centralized vs. Decentralized

It is important to consider process flow and security available at each location. In some cases it may make sense to have the items stored and securely destroyed in a centralized environment.

Third Party Retention and Destruction Services

Another consideration for storage and destruction is a third party service. There are several companies that will pick up your items, store them according to your instructions and then securely destroy the items.

Inspection of Checks

Because the scanned image of the physical check becomes the legal document it is important to inspect both the physical check items and check images once they are captured. Some physical security features on the actual checks, such as watermarks, may not survive the imaging process. You may also want to establish a process for examining physical checks prior to transmission to the bank to verify inclusion of critical information such as payee name, amount, and signature and MICR line. Typically, once the original check is imaged and securely stored, agency staff will not access those original images unless there is a question regarding image quality.

Separation of Duties

- Agencies should follow DAS internal controls, revenue [OAM 10.30.00](#)
- For internal fraud prevention, it is advisable to have separation of duties with respect to the deposit process. Remote deposit allows for greater separation of duties than traditional physical deposit. For example, you could allow one employee to complete the check scanning process, but require a separate employee to actually send the batch to the bank.

Batch Preparation

- Separate checks in batches of 100 or less and by check size (i.e., personal vs. business) to increase scanner read rates and reduce time spent on reconciliation errors.
- It is recommended that checks be endorsed prior to being deposited.
- Create procedures for handling items that cannot be electronically deposited, such as cash and foreign checks.
- Educate staff on the extended deadlines with RDC deposits. By depositing on the same day checks are received, agencies may see an increase in their average daily balances for agency accounts.
- Consider the frequency of sending batches to the bank. Most agencies currently using RDC are scanning in multiple batches throughout the day and depositing one time at the end of the work day.
- Determine if types of work should be sorted and deposited in separate batches. For example, you may want to create separate groupings for check-only, check with one coupon, and multiple check / one coupon. You may also consider grouping all checks with the same dollar amount together to speed data entry.
- Just as with physical deposits, agencies utilizing RDC will also see returned items due to NSF and a variety of other reasons. It is recommended that each agency review returned item procedures and determine a process that meets the needs of the agency and their customer. Some agencies will request the bank to redeposit the returned item through two more times and others may want to manually handle all returned items.

Bank Account Control/Treasury Management

- Consider the possibility of eliminating low volume wholesale lockboxes.
- Consider sharing image archive access with other departments, e.g., accounts receivable, in order to prevent unnecessary copying checks.
- Maintain workstations, including laptops that process financial transactions with up to date operating system and security patches.
- Consider limiting internet access on workstations or laptop devices that process banking transactions.
- Remittance file information provided by RDC providers may contain personally identifiable information, (e.g. a consumer bank account number and bank routing number together are considered personally identifiable information under the Oregon Identity Theft Act). It is recommended that state agencies receiving remittance data from the RDC providers ask the provider to omit the Bank Account and Bank Routing number from the remittance data. If there is a business case for including the banking information, it is recommended that agencies have a process for identifying and protecting personally identifiable information stored on agency servers or contained in hard copy reports.