MARYLAND STATE TREASURER

Dereck E. Davis
State Treasurer

Jonathan D. Martin
Chief Deputy Treasurer

Policy on the Use of Remote Deposit Capture Services by Maryland State Agencies

1.0 Objective

The Treasury Management, Banking Services Unit of the Maryland State Treasurer's Office (STO) has issued this Policy on the Use of Remote Deposit Services by Maryland State Agencies (Policy) to provide guidance when utilizing remote deposit capture services (RDC) as a method of making check deposits into the State's bank accounts.

The goal is to provide State agencies with operating policies that will address the unique risks associated with making deposits via RDC. Agencies must comply with the Comptroller's requirements on cash receipt & check handling as outlined in the ***GAD Accounting Policies and Procedures Manual***, as well as guidance per their ***Internal Control Manual for Use by State Departments and Independent Agencies*** for all deposits including RDC.

2.0 Applicability

This Policy applies to all State of Maryland agency locations that utilize RDC to make check deposits to their depository bank accounts.

3.0 Authority

The Treasurer's authority as custodian of State funds and as the Constitutional Officer responsible for the deposit and disbursement of State funds is found under Article VI, Section 3, of the State Constitution and Titles 6 and 7 of the State Finance and Procurement Article of the Annotated Code of Maryland. It is the overall mission of the Treasury Management Division, Banking Services Unit to provide efficient, accurate, and timely banking services to all State agencies and external customers. As part of its overall mission the Treasury Management Division serves as the State's authority for the development, control, and maintenance of statewide policies and procedures for banking products and services.

4.0 Introduction and Rationale for the Policy

Passage of the Check Clearing for the 21st Century Act (Check 21 Act) in 2004 coupled with the advancement of technology has resulted in banks offering customers RDC. RDC is a service that allows bank customers to scan and capture images of bank deposits and present them electronically to the bank without having to physically deliver the check to the bank. From the customer perspective, RDC can eliminate courier and transportation costs and provide quicker access to funds. However, RDC also brings with it inherent risks and challenges as the customer has now taken on new responsibilities that were previously performed internally to the bank (i.e. scanning checks, storing checks, and destroying checks).

This Policy provides State agencies guidance designed to deal with the risks associated with using RDC. State agencies should incorporate this policy guidance into their internal control procedures to ensure the risks of RDC are properly monitored and controlled.

5.0 Remote Deposit Capture Risk Mitigation Policies

5.1 RDC scanners and the host computers for the RDC software shall be located in a secure building or office.

5.2 Agencies are responsible for ensuring that the host computers for RDC scanners have updated anti-virus software. Only State issued computers shall be used for RDC scanning.

5.3 Agencies shall refer to the Comptroller's requirements on cash receipt & check handling as outlined in their ***GAD Accounting Policies and Procedures Manual***, as well as guidance per their ***Internal Control Manual for Use by State Departments and Independent Agencies*** for guidance on user roles, proper handling and processing of receipts, and recordation of deposits in Rstars.

5.4 RDC User Roles:

- Access to the RDC online portal shall be controlled by an agency administrator who shall designate user roles and functions to a limited number of staff with segregated duties.
- Designated users shall be assigned individual user IDs and passwords that shall not be shared among users.
- The person who scans the checks should be independent from the person who prepares the deposit ticket.
- Employees may have more than one role in the deposit process however the roles cannot be consecutive. This includes employees serving as backup support.

5.5 Received checks shall be restrictively endorsed with a stamp and logged immediately upon receipt by the individual who first handles the check. To the extent possible, transfers and handling of checks should be kept to a minimum and should be documented with individuals verifying what is being received.

5.6 Received checks shall be stored in a secure, locked location accessible only to personnel designated to handle checks before, during and after scanning until they are destroyed.

5.7 The agency shall verify that the scanner's spray line (on the physical check) and the virtual endorsement (on the image) are properly added for each scanned check.

5.8 Deposit Tickets:

- Although deposit tickets are not scanned into the Wells Fargo portal, they must be prepared accurately for each deposit to ensure the deposit is associated with its own 'unique' and 'sequential' deposit ticket number.
- The ten-digit deposit ticket number included in the MICR line, which is a combination of the location and deposit ticket number, is required and must be entered into the Wells Fargo portal 'Desktop Deposit' prior to scanning checks.

- The designated State Agency User must input and is required to enter the ten-digit deposit ticket number for each 'Desktop Deposit' transaction. This ensures that the Banking Services Unit can effectively identify deposits and reconcile them between R*Stars and the bank.

- The unique Deposit tickets, which reflect the ten-digit deposit ticket number included in the MICR line, can only be ordered through Superior Press. Order forms can be found on our website.

- State Agencies must not use the "regular deposit tickets" located within Wells Fargo Bank branches. Only unique Deposit Tickets ordered through Superior Press should be used.

5.9 Any checks identified as a duplicate, i.e. included within a prior deposit, shall be removed, and placed with the correct and previously batched deposit. Each occurrence of an identified duplicate shall be documented.

5.10 Deposits should be posted to R*Stars in accordance with the Comptroller of Maryland's "GAD Accounting Procedures Manual," using the five-digit deposit ticket number from the Depository Account deposit ticket. For some agencies this is a six-digit number.

5.11 Per GAD's Accounting Policies and Procedures Manual, monthly bank reconciliations should be performed by someone independent from the initial receipt, deposit ticket preparation and RDC process.

Reconciliations should confirm that;

- Deposits posted to R*Stars/GL tie to the bank;
- Checks documented on the cash receipts log were deposited to the bank;
- Deposit ticket numbers used are in chronological order, with any gaps or changes in sequence accounted for or that there is a reasonable explanation provided;
- Should clearly list checks received but not yet deposited during the month;
- Should clearly list checks deposited but not posted to R*Stars/GL;
- Should verify that checks deposited via RDC that should have been destroyed per section 5.13 have been destroyed by confirming that the shredding date is documented.

5.12 Scanned checks whose transmitted images have been accepted by the bank shall be immediately stored in a secure location until they have been reconciled to the month end statement.

- Checks should be stored separately by month until they are destroyed (to prevent checks from being commingled with cleared and un-cleared checks.)
- The bank may require that a check be rescanned, so agencies should not mark up the face of the check. Note: Checks marked void cannot be rescanned. Please be sure to maintained documentation of such requests for reconciliation and audit purposes.

5.13 Scanned checks shall be destroyed using a crosscut shredder or equivalent secure destruction method.

- Checks should be destroyed one month after they have cleared on the bank statement. For example, if a check clears the bank on the January statement, it should not be destroyed until the February reconciliation has been completed and confirmed that the check was not returned.
- A log of scanned checks on hand should be maintained for tracking dates of destruction and employee initials who destroyed the checks. If feasible, a second employee should witness the destruction of checks, also signing or initialing the log. NOTE: As mentioned in 5.11, this log should be reviewed monthly as part of the reconciliation process.

6.0 Adherence to the policy

It is critical that agencies follow the prescribed procedures outlined in this policy. Specifically, agencies must ensure that;

- Check images are captured clearly to prevent return items from the bank.
- Deposit ticket numbers are keyed correctly in the appropriate field on the Desktop Deposit portal.
- Deposits are keyed timely into R*Stars as outlined in the Comptroller's ***GAD Accounting Policies and Procedures Manual*** with the deposit ticket number referenced in the Document Reference Number field.
- Appropriate segregation of duties has been established or additional controls are in place to ensure all receipts are accounted for.

Agencies that do not follow these procedures on a continuous basis may lose the right to use Remote Desktop Services for processing their deposits, at the discretion of our Office.

Original Date Issued: June 15, 2010
Revised: February 17, 2015
Revised: August 9, 2024

Issued by: *Kimlloy Broughton*
Kimlloy Broughton
Director, Treasury Management