

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

### **1.0 Objective**

The Banking Services Division of the Maryland State Treasurer's Office 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.

### **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 the State Treasury 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 Banking Services Division to provide efficient, accurate, and timely banking services to all State agencies and external customers. As part of its overall mission the Banking Services 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 21<sup>st</sup> 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 checks for deposit 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 new risks and challenges as the customer has

now taken on new responsibilities that were previously performed internal 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 in order to ensure that 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 The host computers for the RDC online portal access shall be loaded with working and up to date anti-virus software.
- 5.3 Access to the RDC online portal shall be controlled by the agency administrator who shall designate user roles and functions to a limited number of staff with segregated duties.
- 5.4 Designated users shall be assigned individual user IDs and passwords that shall not be shared among users.
- 5.5 Received checks shall be restrictively endorsed with a stamp and logged in upon receipt.
- 5.6 Received checks shall be stored in a secure 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 Although deposit tickets are not scanned into the Wells Fargo system, they should be prepared 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 is a combination of location and deposit ticket number and must be entered into the Wells Fargo CEO portal "Desktop Deposit" prior to scanning checks. This ensures that Banking Services can effectively identify deposits and reconcile them between Rstars and the bank. Deposit tickets, using the Treasurer's Office online form, shall be ordered through "Superior Press".
- 5.9 Any checks identified as a duplicate, i.e. residing within a prior deposit, will be removed and placed with the correct and previously batched deposit. Each occurrence of an identified duplicate shall be documented.
- 5.10 The person who scans the checks for deposit should be independent from the person who prepares the deposit ticket.

5.11 Monthly bank reconciliations should be prepared by someone independent from the deposit ticket preparation and RDC process.

- Reconciliations should confirm
  - Deposits posted to R\*Stars/GL tie to the bank;
  - Checks documented on the cash receipts log were deposited to the bank;
  - 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 5.14 have been destroyed by confirming that the shredding date is documented.

5.12 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 Wells Fargo Depository Account deposit ticket. For some agencies this is a six digit number.

5.13 Scanned checks whose transmitted images have been accepted by the bank shall be 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 that are marked void cannot be rescanned.

5.14 Scanned checks shall be destroyed using a cross cut 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 should be maintained tracking dates of destruction and employee initials responsible for destruction of the checks.

Original Date Issued: June 5, 2010

Revised: December 16, 2019

Issued by:           *n clark*            
Nancy Clark  
Director, Treasury Management