SCHEDULE A
Remote Deposit Capture (RDC)
Customer Site-Best Practices

Company

1. If the company terminates the usage of RDC, company will be required to notify the Bank in written form or term customer can contact a branch manager and have them submit the request to E-Banking stating this intention, including planned effective date of termination.

Employee Access

1. Access to the RDC application should be made available only to authorized employees.
2. Each employee should be required to have their own individual user ID and pass code and should never share these items with another employee.
3. When an employee's employment is terminated, the company should immediately remove access to the RDC application for that employee.
4. It is recommended that employees use strong passwords.
5. The bank should be notified if an employee changes duties or leaves the organization.

Physical Access

1. The RDC personal computer and scanner should be located or stored in a secure location.
2. Scanners can be stored away from the RDC personal computer when not in use.

Check Processing

1. The protection of the customer checks throughout all stages of the RDC process is extremely important; the checks being processed may contain confidential customer information.
2. Have procedures in place to secure checks that have already been processed so they are not re-processed thru the RDC application. Verify that checks previously processed are being encoded on the back of the check.
3. It is always good practice to have two individuals verifying the check deposit.
4. Scanned checks should be retained in a secure location after imaging for 3 full months.
5. It is recommended that the company destroy imaged checks by an approved form of document destruction after the pre-approved document retention time period has been reached.
6. Deposits should be reconciled by a party not involved with the deposit process.

Equipment Maintenance & Security

1. Personal computer and check scanner should be located in a clean, climate controlled location.
2. Regular scanner maintenance should be performed per the instructions previously provided.
3. We recommend that you implement and maintain current Anti-Virus/Internet security software and Microsoft critical security patches for Windows Operating Systems.

4. We recommend setting Anti-Virus/Internet Security software to download signature updates daily. You should also ensure real-time protection is activated and schedule a complete system scan of all files at least weekly.
5. We require the use of the Microsoft based operating system and you should also automatically download and install all critical Microsoft security patches as soon as they are available.
6. We recommend the use of network or PC based firewalls.
7. Central Bank employs an IP-based filter from within the Internet Banking application which only allows access from the known customer IP. Any customer not employing a static IP to comply with this standard will be required to sign a waiver document acknowledging acceptance of their increased processing risk.