Remote Deposit Capture and Mobile Deposit Capture Procedures and Measures

Luther Burbank Savings ("LBS" or the "Bank") offers Remote Deposit Capture (RDC) service via Business Online and Mobile Deposit Capture (MDC) service available via the LBS business banking app. The administrator and business' employees are responsible for safeguarding the physical and digital security of all materials and equipment required to process check deposits using these services. The guidelines below are best practice recommendations and should be considered when establishing your own processes. If either service has been requested, you will receive notification via email from the cash management team advising you of your application's approval status and any applicable limits.

If you have any questions about these procedures or need additional guidance, please call 888.578.4495, Monday – Friday, 9am to 5pm (PST), or email onlineaccounthelp@lbsavings.com. When emailing, please do not include any sensitive information such as account number, PIN, password or online ID. You must also contact us immediately if you or your employees become aware of any loss, theft or unauthorized use of RDC or any related information.

General Guidelines for RDC

RDC scanners provided or approved for use with LBS Business Online services can and must only be used for business banking purposes. Use the following guidelines to ensure safe and secure use of services:

- Establish internal procedures outlining how checks will be collected, deposited, safeguarded and destroyed. Loss of information increases the risk of exposing personal, non-public information to unauthorized individuals.
- Establish a secure area to store checks during the retention period.
- Identify users who are authorized to submit RDC transactions, safeguard checks during the retention period and destroy checks.
- Train authorized users in the proper use of services as well as maintaining the physical security of all materials

The Bank may conduct periodic site visits of RDC locations to ensure security and controls are aligned for use of these services.

Safeguarding and Maintaining RDC Equipment

Follow these steps to ensure the scanners are in working condition to avoid process interruptions:

- Keep the scanners in a secure location away from public or unauthorized access.
- Only authorized employees should have access to the scanner. Ensure that authorized employees have training in the proper use of the scanner.
- Maintain the scanners regularly by following the instructions provided with your scanner.
- Replace the ink cartridge when needed.
- Report any malfunctions immediately to avoid service delays.
- Keep your network, desktop operating systems and anti-virus software up to date.
- Ensure the image quality of the scanner is decent for the purposes of reading the check, including the amount, payee, signature, date, and item number, as well as the MICR line items.

Check Safekeeping and Destruction for RDC

You are solely responsible for the safekeeping, retention and destruction of items scanned using RDC. We recommend establishing a control log to track the deposit, retention and destruction of all checks.

Making an RDC Deposit – Establish internal controls to track and deposit checks using RDC.

- Maintain control logs which identify all items deposited in one batch.
- Limit the number of employees who have access to and store checks prior to deposits made.
- Review deposited batches to ensure all logged checks were properly scanned.
- Establish dual control processes for scanning and reviewing checks.

Check Storage – You are required to store checks for a period of thirty (30) days from deposit date.

- Label all physical checks included in a deposit batch once the transaction is processed. Include the deposit date and batch number for easy retrieval of checks if they are requested by the Bank for additional review. Also note the destruction date for checks. You may print a detailed report to keep with checks (available in Business Online).
- Once checks are clearly labeled, they should be stored in a fireproof, locked cabinet or vault. Access to the storage area must be restricted. Limit access to other employees, vendors and guests of your business.

Destruction of Checks – At the end of the 30-day retention period, all checks must be destroyed using a shredder or by engaging off-site destruction services.

For On-site Destruction:

- Refer to the control logs to identify which batches need to be destroyed.
- Validate the label on the batch.
- Shred all checks in the batch using a cross-cut scanner.
- Log the destruction date in your control logs.

For Off-site Destruction:

- Ensure your vendor continues to maintain its certification.
- Schedule regular pick-up of the security containers.
- Refer to control logs to identify which batches need to be destroyed and validate the batch label.
- Record the destruction date after placing the batch in a security container.

Check Safekeeping and Destruction for MDC

- You are solely responsible for the safekeeping, retention and destruction of checks deposited through MDC.
- Checks must be stored securely and retained for 30 days from the deposit date.
- Do not store images of deposited checks on your smartphone.
- Shred checks at the end of the retention period.