

REMOTE DEPOSIT CAPTURE ^{RDC} AND MOBILE REMOTE DEPOSIT CAPTURE ^{mRDC} BEST PRACTICES REFERENCE GUIDE



Controls That Matter Most:

- Use unique user IDs, multifactor authentication, least-privilege access and prompt removal of access when duties/functionality/users change
- Inspect every check prior to scanning, use the institution-required restrictive endorsement and confirm the item is legible before scanning
- Balance the batch, review the image quality, review the dollar amounts and save the submission confirmation
- Prevent duplicate deposits by marking processed items, reconcile daily, retain originals securely for the required period and destroy originals securely
- Escalate suspicious items, duplicate deposits, lost checks unauthorized access or unexplained differences immediately

Institution-Specific Requirements:

Required	Description
Daily Limit	Refer to Approved Daily Limit with Treasury Management
Processing Cutoff Time	5pm CST
Required Endorsement (applicable for mRDC)	FOR MOBILE DEPOSIT ONLY
Treasury Management Support	TreasurySupport@sfbank.com
Original check retention period	60 days
Remote Deposit Capture Endorsement	SFB utilizes Virtual Endorsement – No “physical” endorsement is needed

Before Initial Use of Remote Deposit Scanning Services:

People & Access

- Assign a primary RDC Administrator and a backup. Document who may scan, approve, reconcile and manage users.
- Each authorized user will be given their own individual credentials. Never share user IDs, passwords, tokens or authentication codes.
- Use the minimum access needed. Separate deposit preparation duties from approval/reconciliation duties when staffing permits.
- Review user access at least annually (recommend quarterly) and immediately following a user role change. Alert bank's Treasury Support team as early as possible post-user role change.

Workstations/Scanner/Network

- Use a company-managed device with supported software, current security patches, anti-malware protection, screen locks and encrypted storage.
- Use a trusted business network. Avoid public Wi-Fi. Avoid unapproved remote-access tools.
- Place the scanner and physical checks in an area accessible only to authorized staff.
- Verify software or scanner updates through an approved channel; do not act on unsolicited calls or links claiming to be provide RDC support.

Written Procedures and Training

- Document the complete process of Remote Deposit Capture/Scanning Services: receive checks, inspect checks, endorse checks (when applicable), scan checks, verify scanned totals, submit batch, reconcile, securely store original checks, research/review checks as needed and destroy original checks after applicable retention period.
- Train primary and backup users before they receive access. Refresh training periodically.
- Train users specific to duplicate presentment. A check deposited through RDC/mRDC must never be deposited again at a branch, ATM, through mobile deposit or at another financial institution.
 - Only if the previous scanned check was deemed unable to be processed via Remote Deposit Capture, can that same check be deposited manually at the financial institution.

Controlled Workflow of Remote Deposit Scanning:

- Prepare the Work Area – Secure unrelated documents, verify the approved workstation and scanner and sign-in using your own credentials
- Inspect Each Original Check – Confirm the payee, date, numeric and written amounts, signature, MICR line and visible alterations. Follow the approved rules for stale-dated, post-dated, third-party and foreign items.
- Endorse Exactly as Required – Use the institution approved restricted endorsement and any required client identifier.
- Build and Balance the Batch – Create a deposit listing/generate daily deposit report. Compare the expected count and total to the RDC batch.
- Scan and Review Every Image – Check front and back legibility, orientation, cropping, MICR capture, endorsement visibility and encoded amount. Void and rescan rather than accepting a weak image.
- Approve and Submit – Use dual approval when required.
- Save Evidence – Retain the confirmation or Batch ID and the depository report/summary according to your record-retention policy.

Do Not Submit Batch When:

Stop Condition	Required Response
Item(s) appear altered, counterfeit, incomplete or inconsistent	Quarantine the item(s) and follow your fraud procedure
The system warns of a possible duplicate	Research the item and prior deposits before proceeding
The batch will exceed the daily limit	Contact Treasury Management
The account, amount or image cannot be verified	Correct the issue before submission or remove the item from the batch
The device, credentials or session may be compromised	Stop processing, disconnect as directed, and report the incident immediately

After Batch Submission:

Prevent Duplicates and Protect Originals

- Mark each processed check using the approved method without obscuring information needed for research.
- Store originals in a locked, access-controlled location. Organize the originals by deposit date/batch.
- Do not make deposited checks available for redeposit. Limit access to originals.
- After the institution-required retention period and after confirming final processing, destroy original checks using an approved secure-destruction method such as cross-cut shredding or a documented destruction service.

Daily Reconciliation

- Compare the RDC confirmation to the internal deposit listing and expected accounting entry.
- Review accepted, rejected, adjusted and returned items. Document and resolve differences promptly.
- Confirm the deposit posted to the intended account and investigate unexpected holds or missing credits.
- Keep evidence the above review according to your record retention policy.

Fraud/Security/Privacy:

Red Flag	Why It Matters/Action
Unexpected change to payee, amount, check stock or MICR information	Possible alteration or counterfeit; stop and escalate
Pressure to deposit immediately or bypass review	Possible social engineering; follow procedures
Repeated duplicates reversals, adjustments or unusual return activity	Possible process failure or fraud; track and investigate
Login alerts, unfamiliar users, changed limits or unexpected device prompts	Possible account compromise, report to Treasury Management immediately
Checks left unsecured, missing, photographed or removed from the work area	Possible privacy and redeposit risk; treat as an incident

When/If an Incident Occurs:

- Stop the affected activity; do not delete logs, confirmations, emails or images that may support the investigation
- Notify your financial institution's Treasury Support Team using a verified channel.
- Record who discovered the issue, when it occurred, affected users/devices, bath IDs, check details and actions taken.
- Change credentials or isolate equipment only as directed by your approved internal incident-response process.

When/If an Incident Occurs:

Frequency	Control
Every Deposit	Inspect, endorse, balance, image-review, submit, confirm and secure originals
Daily	Reconcile submitted batches, posting, exceptions, returns and adjustments
Weekly	Review unresolved exceptions and confirm retained checks remain secure
Monthly	Review limits and volumes for unusual patterns. Test backup user readiness.
Quarterly	Review users, roles, devices, procedures and training needs
Annually	Revalidate the RDC process, business continuity, retention/destruction controls and agreement updates. Review and complete financial institution's RDC Questionnaire and Schedule C.

Business Continuity:

- Maintain an approved plan for scanner, workstation, network, power, staffing or service outages.
- Keep current support numbers and account information available through a secure method that does not depend on the affected device.
- Do not use an unapproved personal device, scanner, email account or cloud-storage service as a workaround.
- Track all items handled through the fallback method and reconcile them before resuming RDC.

Remote Deposit Capture Administrator Self-Assessment:

- All Remote Deposit Capture Users have separate/individual login access
- Primary and backup users have completed current training
- The workstation, scanner, network and physical work area meet company security standards
- The required endorsement, eligible-item rules, limits, cutoffs, retention period and support contacts are documented
- Deposits are balanced, image-reviewed, confirmed and reconciled daily
- Original checks are secured, tracked and destroyed according to policy
- Duplicate warnings, exceptions, returns, adjustments and suspicious activity are investigated and documented
- Business continuity and incident escalation procedures are current and are reviewed within the past year

The RDC/mRDC Best Practice Reference Guide does not replace your Remote Deposit Capture Agreement, operating instructions or check handling policies.