REMOTE DEPOSIT CAPTURE

HELP PROTECT YOUR BUSINESS AND YOUR CLIENTS

ALERUS

When utilizing remote deposit capture, it is important to consider the following to help protect your business and your clients from fraud.

Original Checks

- Inspect and verify the quality of check images and ensure they are eligible for all posting and clearing purposes.
- Store original checks for a minimum of 14 days and a maximum of 45 days.
- Keep checks secure (locked) to ensure they are not accessed by unauthorized persons.
- Do no duplicate original checks or store client account information in general files.
- Checks must be shredded and disposed of properly to ensure checks are no longer readable or capable of being reconstructed.

Returned Checks

- Re-depositing returned item — never rescan an original check; wait to receive the image replacement document (IRD). If you have a returned deposit item that can be redeposited, (e.g., NSF first time, missing endorsement, etc.) you MUST wait to receive the IRD. This document is the new original check.
- If you are unsure if you can redeposit a check, contact the treasury management solutions center at 800.279.3200 or **treasury@alerus.com** for assistance.

Security

- Do not share your unique user ID and password.
- Maintain fully qualified, properly trained and experienced administrative staff and employees to sufficiently perform obligations.
- Implement internal controls and procedures to ensure that terminals used to access RDC are attended only by authorized users while accessing such service and that sessions are fully terminated when authorized use is completed.
- Stay updated with the latest updates for your computer operating system and browser. Your systems should be fully patched for critical security issues.
- Install and implement any changes and upgrades to the software and equipment as required by bank within five business days to ensure compliance with regulatory changes or developments, or to protect the integrity and security of the service.
- Implement all commercially reasonable security procedures to control access to computer systems and to protect any data files stored thereon. (Including but not limited to anti-virus and threat prevention; detection and response programs; firewall; proxy servers; and physical, logical, and network security control systems and devices.)

This list is not all-inclusive, but by following these guidelines they can help you protect your business and clients from cyber threats and maintain a secure environment for your operations.