

Remote Deposit Capture shifts the deposit function from the bank to the customer, introducing risks such as poor image quality, duplicate deposits, and the security of non-public customer information (NPI). NPI includes details like account and routing numbers, addresses, phone numbers, dates of birth, driver's license numbers, and tax identification numbers, often found on checks handled by merchants. Securing this information is crucial to prevent unauthorized access and potential fraud.

- Implement a change management process for software and device updates.
- Restrict "Administrator" privileges for employees.
- Use a firewall on the network.
- Deploy an Intrusion Detection System (IDS).
- Filter internet content on the network.
- Secure wireless technology accessing banking services.
- Limit use of banking services outside the network.
- Use a spam filter for email clients.
- Regularly update Java and Flash applications.
- Use dedicated devices for banking services.
- Assign personnel to manage user access to Inwood services.
- Avoid downloading/retaining non-public information.
- Secure any retained non-public information.
- Ensure physical security controls at the facility.
- Obtain cyber or internet liability insurance.
- Have a breach notification procedure.
- Require employees to sign an Acceptable Use Policy (AUP).
- Train employees on computer, internet, and email security.
- Conduct background checks before hiring.
- Prevent duplicate presentment of checks.
- Inspect and clean equipment for quality images.
- Securely store scanned checks.
- Do not retain scanned checks beyond 30 days.
- Destroy scanned checks after the retention period.

This tool assists business owners and principals in identifying, understanding, measuring, and mitigating risk. Please note, it is not a comprehensive list of actions to take.

INWOOD NATIONAL BANK Member FDIC