Apple Financial Holdings, Inc.

IT Remote Deposit Capture Procedures

August 24, 2021

Contents

PROCEDURES NAME: IT Remote Deposit Capture Procedures

REVIEW AND TRACKING CHART

Effective Date*:	August 24th, 2021
Version Number:	3.6
Review Frequency:	Annual (Every 12 Months)
Last Review Date*:	August 2021
Next Review Date*:	September 2022
Business Area Leader:	Debit Gupta, EVP Chief Technology Officer
Overarching Policy or Policies:	Consumer Banking Business Remote Deposit Capture
Procedures Owner:	Rajesh Kalyanaraman, FVP Digital platform/Channel, Bus Services, Loan tech support

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Information Technology Remote Deposit Capture (RDC) Procedures (the "Procedures") applies to the Implementation & Management of IT processes for servicing the RDC customers at Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank") in accordance with applicable state and federal statutes, rules and regulations.

All Apple Bank employees and third party resources engaged by the Bank must comply with the terms of these Procedures to the degree applicable to them.

II. DEFINITIONS

- **Annual or Annually:** Every twelve (12) months.

- **Chief Technology Officer**: The Chief Technology Officer is responsible for all IT related activities in partnership with RDC vendor including implementation of IT systems such as the hardware and software required for the RDC product, reviewing site security, communicating customer information security procedures and providing training for both internal Bank employees and the end users (or external customers)

- **IT Governance & Change Management**: The management level person who oversees all of IT policies and Procedures, and part of IT procedures approval process.

- **Business Area Leader:** The management level person who is responsible for the Annual review and approval of Procedures and making and tracking any updates thereto.

- **Policies and Procedures Administrator ("PPA"):** The PPA is a member of Risk Management, and in charge of uploading the approved policies, procedures, and manuals onto AppleNet.

- **Procedures Owner ("Owner"):** The point person for the Procedures, who is responsible for keeping track of the required approvals, as well as incorporation of interim changes to the Procedures as circumstances warrant. The Owner could, but is not required to, be same person as the Business Area Leader as defined above. Further the procedure could be the person directly owns the IT Procedures for the RDC processes.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines procedures with respect to the Information Technology RDC Processes (the "Procedures") that apply to the RDC services (as outlined below) for customers at Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank") in accordance with applicable state and federal statutes, rules and regulations.

a. IT On boarding of a new RDC customer onto the FIS DLM [Direct Link Merchant],
b. Installation of software & scanner at the new RDC customer location,
c. Ongoing IT support to the RDC customers consisting of

1. User Administration and
2. Ongoing Maintenance (including customer limit maintenance)

d. Off boarding from the DLM system.

2. Objectives

The objective of these Procedures is to present details of all IT Processes associated with Business RDC services offered to our Apple Bank customers.

3. Key Components of Procedures

This section will detail several key IT processes as outlined above:

3.1 Onboarding / Setup of new customers onto FIS DLM system

After all vetting and qualifying of RDC customers is done by the RAU in Retail Banking – the IT Customer Product Specialist in Digital Operations will receive communication for a new customer setup. Once the RAU communicates that a business customer has been approved – the IT resource will follow the steps as below:

1. Log into DLM system as an administrator (see also 3.3)
2. Under Administration > Merchants, click the "+" icon on the left side above existing Merchants.
3. Under the General Information tab, enter the Display Name of the Company, Tax ID, Live Date, and Available Days of Data as 365. Expand Contact Information and enter the Name, Email, Phone, Address, City State, ZIP Code and Country. On Roles, click the "…" icon to select the roles, Desktop Operator, Researcher and Reviewer and click done. Once completed click Save.
4. Under the Capture tab, on Supported Scanners click the "…" button and select the scanner which the customer has listed on their application and click Done. For Duplicate Detection, select Enable for, Critical for, and enter "365" for History in Days. Once completed click Save.
5. Under the Accounts tab, click the "+" button, enter the Account Number, Display Name (with last 4 of account #), Work Type as 10. DL Merchant, Routing Number as 226070584 (for Apple Bank), enter 10 for Trancode and click Save.
6. Under the Locations tab, under name enter the Location. Expand the Contact Information and enter the Name (admin), Address, City, State, ZIP, and Country. Once completed click Save.
7. Under the Users Tab (for each new user), click the "+" button, enter the User (Login ID), Full Name, Email, Time zone as EST, and select the scanner in the dropdown. Enter the Phone numbers from the application. Under Roles, click the "…" and select, Desktop Operator, Researcher and Reviewer and click Done. Under Locations, click the "…" and select the location and click Done. Under accounts, select the appropriate accounts and click Done. Once completed click Save.
8. Under the Review tab, enter the daily hard limit, deposit hard limit, and item hard limits from the approved application. Enter the Deposit Soft Limit of $24,999.99

as RAU reviews deposits of $25,000.00 and over. (All limits set under Review transfer over to the accounts as Inherited). Under Review Settings, select Bank and check the box for Enable Review. Expand Amounts Exceeded and check the box for Item Soft Amount Exceeded. Once completed click Save.

3.2 RDC Equipment Installation & Training

The IT Customer Product Specialist or designated authorized person will arrange for a training and installation date with the new RDC customer (& if needed in partnership with the FIS Support team).The Branch Manager or designated person from the Retail Risk analysis unit may accompany the IT Customer Product Specialist or designated authorized person, but it is not required.

- Contact the customer via email/phone as an introduction and to determine best available dates for installation.
- Provide user credentials (Login ID and temp pw) as well as DLM URL to each new user and walkthrough their initial login process.
- During the initial login process, the end-user is prompted to setup Multi-Factor Authentication with the phone number of their choice (mobile recommended). If during the login process, the User decides to register their device, a cookie is then stored on the end-user's machine, so MFA is only triggered again on an unregistered device.
- Create a ticket within the FIS Client Portal to schedule an installation with a support technician at the requested date and time.
- Once coordinated, create a calendar (meet) invite to share with the customer, FIS technician and participating member of the RAU team. Also advise the customer to have IT support available for firewall permissions and have a check ready to scan if possible during training.
- During the installation, the FIS technician will join the customer PC via Bomgar session. This will allow them to install the necessary scanners drivers on the PC to be used for scanning.
- Once the installation is complete, the IT Customer Product Specialist conducts the training process, which consists of a walkthrough of the functionality within the DLM platform (submitting new deposits, correcting exceptions, reviewing deposit reports, and troubleshooting) The end of the session is open to Q&A with the customer as well.
- Once completed, the IT Customer Product Specialist provides the customer with contact information found on the Remote Deposit Service Error Resolution document for any future issues they may encounter, including IT Support and Apple Bank’s dedicated RDC “White Glove Service”.

Following installation and training RDC customer should now be ready to begin scanning.

1. As part of the RDC installation and training, the customer will be provided with contact information should there be hardware or software issues or other questions. The customer will receive a “Remote Deposit Service Error Resolution” form, which will assist RDC customer in resolving issues that may arise.

2. It is more likely however, that initial contact by the customer will be directed to the Branch Manager. The Branch Manager (in partnership with IT) will determine the RDC issues and contact the appropriate area of the Bank for resolution. (e.g., if the customer wants to add additional accounts, the "Remote Deposit Additional Account (s) Request" Form, B-363A will be sent to them. Upon approval, Branch Manager will contact RAU for final approval and forward the request to the IT Customer Product Specialist or designated authorized person to complete the request.)

3.3 User Administration & Support

The IT management & support team has system administrator rights to the DLM system providing access to add and remover users, or disables users, reset users, and reset their password and security questions. RDC customers have limited access and roles. Senior Management has rights to define common roles on the Bank Direct Link Merchant System for each customer based on job functions.

NOTE: Refer to Bank Direct Link Merchant User's Guide for detail user administration and procedures for the following sections:

- About User Administration
- Adding Users
- Working with Existing Users

3.4 Changing RDC Customer attributes including Limits

The IT Product Support specialist in the Digital Operations team or designated authorized person will take the following steps to add accounts or make changes to existing accounts (as directed by Retail Banking). This step happens only after the RAU advises IT that limits have changes, accounts have been added, etc.

- Review form B-363A "Remote Deposit Additional Account (s) request" thoroughly for accurate and complete account information by RDC customer;
- Log onto the AFH's DLM [Direct Link Merchant] System by clicking the icon from your desk top and select the sign in (blue tab) icon;
- Select the administration tab from the menu bar;
- Select the merchant tab from the drop-down list to view the list of merchant account names;
- Select the merchant's name form the drop down list you want to work with to add accounts to or make changes to existing accounts;
- Select the account tab in the menu bar to view selected merchant accounts;
- Select the plus sign from the Search Account or Display Name tab to add accounts or make change to existing accounts;
- IT Product Support specialist or designated authorized person will enter the following RDC customer information;

  a. Account Number

b. Display Name

c. Routing Number

d. Tran code Work Type

- Select the save tab to confirm the account were successfully added;
- Select the user tab from the menu bar to view and grant authorization to primary user's role access the new account(s) added;
- Select the save tab to confirm the primary users have successfully been granted access;
- Select the general information tab from menu bar to repeat the process to add another merchant customer or you can log out by clicking the user icon (👤) in the menu bar and select log out.

Note:

- In general, the RDC service is only available for business accounts however, on a case-by-case basis - Personal accounts belonging to the principal/owner of the entity may be approved. This review and approval process is set forth in the Retail Banking RDC procedures.
- Changes to any of the established customer RDC limits must be made in accordance with Retail Banking procedures & approved documentation, must be received by the IT department prior to implementation of any such limit adjustments.

3.3 Capturing Items

The customer can refer to the latest Bank Direct Link Merchant User's Guide for Capturing, Correcting, Balancing, and reviewing procedures

When the customer is using the using Bank Direct Link Merchant System on a workstation with a scanner, the capture items page provides the customer with a capture button that starts the scanning process.

If the customer already has a compatible scanner, purchase of a new one is not required.

3.5 Off Boarding

Very similar to the on-boarding process highlighted in section A – Retail bank might terminate the relationship with the customer for the RDC service. This termination might be due either the customer requesting the termination (due to variety of reasons including moving the relationship elsewhere) or the bank terminating the relationship due to – as an example – risky behavior by the customer etc.

In either case - as part of the termination process – communication will come to Information technology from Retail banking via the Risk Analysis unit. This termination communication will be in an email form requesting the customer be "off boarded" from the DLM system so as the customer might be prohibited from scanning their work from the effective date of off boarding. At a high level – the customer (or the merchant) and all their users are disabled from the DLM portal. The termination email is kept as a recordkeeping in the RDC folder.

The steps are as follows:

- RAU will communicate the RDC customer off boarding request to the IT Product Support specialist in the Digital Operations team via an email based on their departmental review processes.
- IT Product Support specialist will make the necessary maintenance to the RDC customer's profile within Direct Link Merchant (DLM) in disabling the merchant profile as well as all associated user credentials and advice once completed.
- IT Product Support specialist will maintain email correspondence of the received and completed request in the RDC customer's respective folder along with the DLM Change Audit record as evidence of the merchant and user credentials being disabled.
- In the event that a scanner was provided to a customer on a lending of use basis, the Retail Relationship Manager or District Manager would coordinate in the device collection, which would also be documented via email correspondence by IT Product Support specialist in the RDC customer's respective folder.

4. Escalation Procedures

The Procedures Owner will monitor these Procedures. Any non-compliance with the Procedures will be escalated to the CTO or IT Governance Leader for resolution.

IV. REQUIRED ANNUAL (12 MONTH) REVIEW

The Procedures Owner is responsible for initiating an Annual review of the Procedures. The Procedures Owner will track the review date for the Procedures and begin the review process early enough to provide ample time for the appropriate review to occur in a timely manner. The Procedures do not go into effect until all steps listed below are complete. Steps for required Annual review are as follows:

a) The Procedures shall be reviewed annually by the Procedures Owner, considering relevant individuals and departments to the extent necessary and updated (if necessary).

b) The Procedures shall be submitted CTO and / or head of IT Governance team (and if needed to the Business Area Leader - if different than the Procedures Owner) for approval and no further approval is required. A record of all such changes shall be kept by the Procedures Owner.

Once the steps above are completed, the updated Procedures shall go into effect and the Procedures Owner shall be responsible for delivering the approved Procedures document to the PPA within seven days of the approval date so that it can be loaded in a timely manner to AppleNet or such other intranet site where Procedures are stored and made available to the employees of the Bank.

The Next Review Date shall be adjusted accordingly.

If there are any questions about the above process, contact Corporate Governance at corpsec@applebank.com.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

If the Procedures require changes to be made outside the Required Annual (12 Month) Review outlined in the previous section, the same steps as outlined in the previous section shall apply.

VI. EXCEPTIONS TO THE PROCEDURES

Requests for exceptions to these Procedures must be specific and may only be granted on specific items, rather than to entire sections. The ABS staff will communicate their exception requests in writing to the Procedures Owner, who will then present the request to the CTO/IT Governance (& if needed – to Business Area Leader) for consideration.

VII. ROLES AND RESPONSIBILITIES

- **Chief Technology Officer**: The Chief Technology Officer is responsible for all IT related activities optionally in partnership with RDC vendor including implementation of IT systems such as the hardware and software required for the RDC product, reviewing site security, communicating customer information security procedures and providing training for both internal Bank employees and the end user.

- **IT Governance & Change Management**: The Management level person who oversees all of IT policies and Procedures, and part of IT procedures approval process.

- **Business Area Leader:** The management level person who is responsible for the Annual review and approval of Procedures and making and tracking any updates thereto.

- **Policies and Procedures Administrator ("PPA"):** The PPA is a member of Risk Management, and in charge of uploading the approved policies, procedures, and manuals onto AppleNet.

- **Procedures Owner ("Owner"):** The point person for the Procedures, who is responsible for keeping track of the required approvals, as well as incorporation of interim changes to the Procedures as circumstances warrant. The Owner could, but is not required to, be same person as the Business Area Leader as defined above. Further the procedure could be the person directly owns the IT Procedures for the RDC processes.

- **Risk Analysis Unit ("RAU"):** The RAU that reports to Branch Administration within Retail Banking is responsible for advising IT of all business customers approved for RDC in a timely manner. Additionally, the RAU is responsible for the timely communication to IT of all approved changes to customer RDC limits as well as the addition/deletion of accounts eligible for scanning.

VIII. RECORD RETENTION

Any records created as a result of this Procedures should be held pursuant to the Bank's Record Retention and Disposal Policy. Should records created as a result of this Procedures require a different retention period (either a shorter or longer time period), the Procedures Owner must describe the rationale for a different retention period and share the rationale with the Business Area Leader, who shall in turn document the deviation and supporting rationale in such a way that it can be presented to relevant parties upon request.

IX. QUESTIONS AND CONTACT INFORMATION

Questions regarding compliance with these Procedures may be addressed to the Procedures Owner listed in the tracking chart on the first page.

X. LIST OF REFERENCE DOCUMENTS

- Business RDC policy.PDF
- Retail RDC Procedures.PDF

XI. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
2.0	November 2018		Eddie Deriso	Board
3.0	July-Aug 2019	Enhancement	Rajesh Kalyanaraman	
3.1	Aug 2019	Edits due to Corrections / clarifications sought by Compliance	Rajesh Kalyanaraman	
3.2	Oct 2019	Edits after final review by Compliance& Retail. TPU Renamed as ItemsProcessing & Digital Operations	Rajesh Kalyanaraman	
3.3	May 2020	Edits after RAU unit on behalf of Retail has taken over all of the review process from Items Processing (aka TPU) group.	Rajesh Kalyanaraman	**CTO/IT Governance**
3.4	July-Sep 2020	Edits after Items Processing audit – Off boarding & other process not documented	Rajesh Kalyanaraman/ John Murray	**CTO/IT Governance**
3.5	July-Sep 2020	Final Edits from Business & IT Governance - Lou Dellabovie/ Anthony Scarola/Debi Gupta	Rajesh Kalyanaraman	**Retail/IT Governance**

3.6	8/24/2021	Added verbiage that clarifies multi-factor authentication (MFA) process.	Sam Streeter	**CTO/IT Governance**