Remote Deposit Capture Disclosure & Agreement

This Remote Deposit Capture (RDC) Disclosure & Agreement ("Agreement") applies to Salal Credit Union's ("Salal", "Credit Union") provision of Remote Deposit Capture Services ("RDC") and Mobile Remote Deposit Capture Services ("mRDC"), collectively, the "Services." The Services provide participating businesses with the ability to deposit checks electronically to their enrolled accounts. Use of the Credit Union's RDC or mRDC Services constitutes the acknowledgement of, and agreement to, this Agreement.

The Business should keep a copy of this Agreement for its records.

Terms used but not defined in this Agreement shall have the meanings assigned to such terms in Regulation CC. Terms used but not defined in this Agreement or by Regulation CC shall have the meanings assigned to such terms in the Uniform Commercial Code, as codified in the State of Washington (the "UCC"). The following terms are defined as follows:

- **Account** – The business account(s) at the Credit Union into which deposits will be made.
- **Administrator** – The user assigned on the *Remote Deposit Capture Enrollment* form.
- **Business** – The business named on the *Remote Deposit Capture Enrollment* form.
- **Business Day** – Every day except Saturday, Sunday, and federal holidays.
- **Authorized Equipment** – Equipment that has been approved by the Credit Union for use with the Software.
- **Check** – A draft that is payable on demand, drawn on or payable through or at an office of a United States Financial Institution, whether negotiable or not, and payable to the Business, and includes Electronic Checks, Original Checks, and Substitute Checks. Such term does not include Non-Cash Items (as defined in Regulation CC) or items payable in a medium other than United States dollars.
    - Note: The Credit Union's processing of items that do not meet this definition shall neither constitute a waiver by the Credit Union nor obligate it to process nonconforming items in the future. The Credit Union may discontinue processing of nonconforming items at any time, without cause or prior notice.
- **Coupon or Remittance Coupon** – An item containing information necessary for processing a payment. Example: A payment stub including invoice payment information.
- **Electronic Check** – A digitized image of an Original Check or Image Replacement Document (IRD), as approved by the Credit Union for processing through the Software that may be cleared with a payor's financial institution, with or without the need to convert the image to a "Substitute Check" and:
    - Contains an image of the front and back of the Original Check.
    - Conforms, in paper stock, MICR line information, dimension, and otherwise, with generally applicable industry standards for electronic checks.
    - Is suitable for automated processing in the same manner as the Original Check.
- **Imaged Item, Original Check, or Original Item** – The original paper check used to create the Electronic Check.
- **Image Replacement Document (IRD) or Substitute Check** – A paper reproduction created from the digitized image of a Check with the following characteristics:
    - Consists of an image of the front and back of the Check that accurately and legibly represents all of the information that was on the Check (including the full MICR line), with the exception of color, background designs, texture, pen pressure, and other similar non-textual information that cannot be captured by a digitized representation.
    - Includes the endorsement information for any Person that handled the Check or IRD.
    - If the document is for a returned Check, bears a legend stating the return reason.
    - Is on paper, MICR-encoded to match the MICR line of the Check, and suitable for automated processing in the same manner as the Check.
    - Meets such other technical standards as required under Regulation CC.
- **Indemnifying Credit Union** – A Credit Union that is providing an indemnity under Regulation CC with respect to a Check.
- **MICR** – The numbers, which may include the routing number, account number, Check number, Check amount, and other information, that are printed near the bottom of a Check in magnetic ink in accordance with generally applicable industry standards.
- **mRDC** – All information, web and cellular phone-based services, technological infrastructure, and installed software and applications on the Business or Business user's mobile devices, which allows the Business to submit Checks for deposit through the Credit Union's Software.
- **Payor Financial Institution** – The financial institution ordered in a Check to make payment to the payee(s) named on the Check.
- **Software** – That portion of the software developed, licensed, and/or provided by the Credit Union and its licensors for operation of the Services, that the Credit Union delivers or provides to the Business hereunder.

- **RDC** – All information, web-based services, technological infrastructure, and installed software on the Business's computers, which allows the Business to submit Checks for deposit to the Credit Union. Any references to RDC in this Agreement include mRDC as defined above.
- **RDC Documentation** – All documentation, application forms, manuals, and instructions relating to the Services or the Authorized Equipment which the Credit Union provides to the Business and/or the Business purchases from the Credit Union from time to time pursuant to this Agreement, including, without limitation, documentation regarding installation and use of the Software.
- **Remittance Specification Form** – A form to be used to determine customized scan zones on a Coupon or Remittance Coupon.
- **Single Field Entry** – The ability for the Business to enter free-form information in a data field that is applicable to the specific check image.
- **Web Service** – That portion of the Credit Union's service, through which a Business of the Credit Union may access its accounts through a website, which has been developed, licensed, and/or provided by the Credit Union and its licensors to the Business to be used in connection with the Services.

License

Subject to the terms and conditions of this Agreement, the Credit Union hereby grants the Business a non-exclusive, non-transferable license to:

- Use the Software and/or mobile application for those portions of the Services selected by the Business, solely for processing Checks in connection with the Business's own operations, in accordance with the RDC Documentation and solely on Authorized Equipment.
- Use the RDC Documentation solely to support the Business's authorized use of the Software.
- Copy any Software actually delivered to the Business solely for archival or backup purposes.

Representations and Warranties of the Business

The Business represents and warrants that, with respect to each Check and corresponding Electronic Check processed in connection with the Services:

- The Business is entitled to enforce the Check and Electronic Check.
- All signatures on the Check and Electronic Check are authentic and authorized.
- The Check and Electronic Check are not counterfeit.
- The Check and Electronic Check have not been altered.
- The Electronic Check is a digitized image of the Original Check and accurately represents all the information on the front and back of the Check as of the time the Check was converted to an Electronic Check.
- The Electronic Check will conform to the technical standards set forth in Regulation J and/or Federal Reserve Credit Union Operating Circulars and will allow the Credit Union to create a valid Substitute Check under Regulation CC.
- Neither the Check, nor any Electronic Check or other digitized image of the Check, will be presented for payment such that an endorser, Depositary Financial Institution, Payor Financial Institution, or the drawer will be asked to make a payment twice with respect to the Check, including, without limitation, by placing such restrictive endorsement on Checks, or voiding Checks, as the Credit Union may reasonably require.
- The Check and Electronic Check are not subject to a defense or claim in recoupment of any party that can be asserted against the Business.
- The Business has no knowledge of any insolvency proceeding commenced with respect to the Business, or in case of an unaccepted Check, the drawer.
- The Check is and was at the time of its creation, a bona fide and existing obligation of a debtor of the Business.
- The Business makes all transfer and presentment warranties under applicable law with respect to each Electronic Check to the same extent as if the Electronic Check was a paper Check.

The Business also agrees to comply with the Business Responsibilities outlined in this Agreement.

Limits

The Business will have limits set as defined on the *Remote Deposit Capture Enrollment* form. Limits may be adjusted at the sole discretion of the Credit Union as necessary from time to time. Deposits that exceed the limit will be reviewed and a hold may be placed, the review may result in a delay of the deposit posting to the Account. Limits are subject to change.

- **Per Item Limit:** Total dollar amount allowed for any one check within a deposit.

Fees

The Business will pay the Credit Union the license and service fees as set forth in the applicable *Business Product & Fee Disclosure*. The Credit Union may charge to the account all fees imposed on the Credit Union that are the responsibility of the Business. Amounts owed by the Business will be collected on a monthly basis by the Credit Union. The Credit Union may collect amounts owed by debiting any of the Business's accounts with the Credit Union or by billing the Business. The Credit Union reserves the right to change fees from time to time. The Business will be responsible for any attorney fees or related expenses that the Credit Union may incur when collecting any fees or sums owed by the Business. The Business shall be responsible for and pay all sales and other taxes applicable to this Agreement as imposed by any governmental authority, including, without limitation, any sales, use, and other taxes associated with the Service or Authorized Equipment, except income taxes of the Credit Union, including all applicable excise, property, value-added, sales or use, or similar taxes, any withholding taxes, national pension or other welfare taxes, customs, import, export or other duties, levies, tariffs, taxes, or other similar charges.

Right to Audit

The Business acknowledges and agrees that the Credit Union is authorized to audit its compliance with the terms of this Agreement under the Credit Union's sole discretion. This may include a physical site visit to validate compliance with this Agreement if the Credit Union determines that such a need is required.

Term and Termination

The terms of this Agreement shall commence upon execution hereof and shall continue thereafter until terminated as follows:

- By either party by phone, email, or written notice to the other party, for any reason.
- By the Credit Union upon notice to the Business for the Business's failure to:
    - Pay the Credit Union any amount due to the Credit Union under this Agreement.
    - Install and use any changes or updates to the Software as required herein.
    - The Business fails to provide financial or other information reasonably requested by the Credit Union.
- By the Credit Union immediately if:
    - The Credit Union discovers any willful misconduct (including "bad checks" or fraudulent activities) on the part of the Business or any other party with respect to Checks or Electronic Checks processed by the Business or the Business otherwise violates the terms of this Agreement.
    - If in the good faith opinion of the Credit Union the Business is involved in illegal or unethical business practices.
    - Upon a site survey by the Credit Union or by any determination the Credit Union learns of the Business's non-compliance with security measures.
    - The Business becomes insolvent or files, or has filed against it, any bankruptcy or other insolvency, reorganization, liquidation, or dissolution proceeding of any kind.
    - The Business experiences material or adverse changes to the Business's business or financial condition.
    - The Credit Union determines it is impractical or illegal to provide Services to the Business due to changes in law, rules, or regulations.

Any termination will not affect obligations arising prior to termination, such as the obligation to process any Checks and Electronic Checks, including, without limitation, returned Electronic Checks that were in the process of being transmitted or collected prior to the termination date. Within 30 days after termination of this Agreement, the Business will return or destroy all copies of the Software and RDC Documentation in its possession or under its control, and will, upon request, certify in writing that it has returned or destroyed all such copies. In addition, the Business will keep its Account at the Credit Union open until the later of:

- 60 days after the date of termination.
- Final payment with respect to all processing fees and will keep in such Account an amount sufficient to cover any remaining outstanding Checks. If any such outstanding Checks or returned items exceed the amount in the Account, the Business will pay such excess to the Credit Union upon demand. The Business will also continue to retain Checks and forward Checks to the Credit Union as provided in this Agreement.

All aspects of this Agreement which are intended by their terms to survive termination of the Service, will survive any termination of this Agreement.

Confidential Information

For the purposes of this Agreement, Confidential Information is defined as any information obtained by or disclosed or made available to either party hereto (whether in writing, verbally, or by observation of objects or processes) from or by the other party, that is accompanied by a clear indication that the disclosing party considers the information to be confidential or proprietary, or is of a type that the recipient should reasonably consider it the confidential or proprietary information of the disclosing party or its licensors.

Confidential Information does not include information that:

- Is or becomes generally available to the public other than as a result of a disclosure by the recipient.
- Was in the recipient's possession before the time of disclosure.
- Is or becomes available to the recipient on a non-confidential basis from another source, provided that the recipient has no actual knowledge that the source of such information was bound by and in breach of a confidentiality obligation with respect to such information.
- Is independently developed by the recipient without reference to or use of the disclosing party's other Confidential Information.

Each party acknowledges that it may obtain or have access to the Confidential Information of the other party, and agrees to:

- Maintain the confidentiality, integrity, and security of such Confidential Information.
- Use such Confidential Information only for the purposes set forth in this Agreement, including, without limitation, for the performance of its obligations and exercise of its rights hereunder.
- Disclose such Confidential Information only:
    - To its employees, agents, auditors, accountants, attorneys, and regulators, and only as necessary to perform its obligations and/or exercise or enforce its rights hereunder.
    - If and to the extent necessary to comply with obligations imposed upon it by law.
- Maintain physical, technical, procedural, and administrative controls, and safeguards reasonably designed (taking into account the nature and circumstances of such party's business) to ensure the security, integrity, and confidentiality of Confidential Information, and to protect against any anticipated threats or hazards to the security or integrity of, or unauthorized access to, the Confidential Information, subject to the Credit Union's limited liability as set forth in this Agreement.

The Web Service and the RDC Documentation, and any database, proprietary data, processes, methods, information, or documentation disclosed or made available to the Business as part of or in connection with the performance of the Credit Union's services under this Agreement, shall be deemed the Confidential Information of the Credit Union for purposes of this Agreement. Upon any termination of this Service for any reason, the Business shall return to the Credit Union any and all copies of any Confidential Information within the possession or control of the Business.

The Business acknowledges and agrees that information provided over the Web Service may be processed by third-party service providers. The Credit Union does not warrant the Confidential Information or Services information will be transported without unauthorized interception or modification, or that the Business's account will not be accessed or compromised by unauthorized third parties (e.g., hackers), and the Business holds the Credit Union harmless therefrom.

Changes or Interruptions in Services

The Credit Union may need to perform maintenance, modifications, or updates on its equipment or systems, which may result in interrupted access to the Service or interruptions to or errors in the Service. The Credit Union may also need to change the scope of the Services from time to time. The Credit Union will attempt to provide the Business with prior notice of such interruptions and changes but does not guarantee that such notice will be provided. The Credit Union shall have no liability to the Business for any damage or other loss, direct or consequential, incurred, directly or indirectly, including without limitation any loss of use of business, revenue, profits, opportunity, or good will, even if the Credit Union is aware of the possibility of such damages, which the Business may incur by reason of any such interruptions or errors.

Business Indemnity

The Business will indemnify and hold harmless the Credit Union, its licensors and providers of the Services, and their respective directors, officers, shareholders, employees, and agents, against any and all third-party suits, proceedings, claims, demands, causes of action, damages, expenses (including reasonable attorneys' fees and other legal expenses), liabilities, and other losses resulting from:

- The wrongful acts or omissions of the Business, or any person acting on the Business's behalf, arising in connection with the Business's use of the Services or processing of Checks hereunder, including, without limitation:
    - A breach by the Business of any provision, representation, or warranty of this Agreement.
    - The negligence or willful misconduct (whether by act or omission) of the Business, its users, or any third party on behalf of the Business.
    - Any modifications or changes to the Software made by the Business or any third party within the control or on behalf of the Business.
    - Any misuse of the Services by the Business or any third party within the control or on behalf of the Business.
    - The failure by the Business to comply with applicable state and federal laws and regulations.
    - Any failure by the Business to prevent the loss or theft of a Check or to prevent a Check, digitized image of a Check, or Electronic Check from being presented for payment more than once.
    - Any failure by the Business to void a Check properly.
- Any act or omission of the Credit Union that is in accordance with this Agreement or instructions from the Business.
- Actions by third parties (such as the introduction of a virus) that delay, alter, or corrupt the transmission of an Electronic Check to the Credit Union.
- Any damage to the Business's Information Technology infrastructure due to incompatibility with the Services.

The Business will indemnify and hold harmless the Credit Union and any subsequent recipient of the Electronic Check (including a collecting or returning financial institution, the drawer, the drawee, the payee, and any indorser—collectively "Recipients") for any loss incurred by Recipients if that loss occurred due to the receipt of a Substitute Check or Electronic Check instead of the Original Check. This provision shall survive termination of this Service.

Disclaimer of Warranty

The Services are provided on an "as is," "as available" basis. The Credit Union does not make any warranties as to the use of the Services or with respect to any equipment, hardware, software, or internet provider service. The Business expressly acknowledges that the Services are computer network-based services, which may be subject to outages, interruptions, attacks by third parties, and delay occurrences. In such an event and subject to the terms hereof, the Credit Union will use commercially reasonable efforts to remedy material interruptions and will provide adjustments, repairs, and replacements, within its capacity, that are necessary to enable the Services to perform their intended functions in a reasonable manner. The Business acknowledges that the Credit Union does not warrant that such efforts will be successful. If the Credit Union's efforts are not successful, the Business may terminate this Service(s). The foregoing will constitute the Business's sole remedy, and the Credit Union's sole liability, in the event of interruption, outage, or other delay occurrences in the Services. The Credit Union does not warrant the services of any third party, including, without limitation, the Business service provider or any third-party processor.

Credit Union's Liability

The Credit Union will not be liable for any of the following, unless liability of loss is a result of the gross negligence, willful misconduct, or failure to exercise ordinary care by the Credit Union:

- Any damages, costs, or other consequences caused by or related to the Credit Union's actions that are based on information or instructions that the Business provides to the Credit Union.
- Any unauthorized actions initiated or caused by the Business or its employees or agents.
- The failure of third parties or vendors to perform satisfactorily.
- Any refusal of a Payor Financial Institution to pay an Electronic Check or Substitute Check that was allegedly unauthorized, was a counterfeit, had been altered, or had a forged signature.
- Any other party's lack of access to the internet or inability to transmit or receive data.
- Failures or errors on the part of internet service providers, telecommunications providers, or any other party's own internal systems.

- Any of the matters described under the 'Business Indemnity' section.

The Credit Union's liability for errors or omissions with respect to the data transmitted or printed by the Credit Union will be limited to correcting the errors or omissions. Correction will be limited to reprinting and/or representing Substitute Checks or Electronic Checks to the Payor Financial Institution. In no event will clerical errors or mistakes in judgement be constituted as failure to exercise ordinary care.

Notwithstanding anything to the contrary in this Agreement, the Credit Union's aggregate liability to the Business for claims relating to this Service, whether for breach, negligence, infringement, in tort, or otherwise, and arising during any twelve-month period, shall be limited to an amount equal to the total fees paid by the Business to the Credit Union for such twelve-month period.

In no event will either party be liable for any consequential, indirect, incidental, special, or punitive damages, or any lost profits or loss of any opportunity or good will, even if such party has been advised of the possibility of such damages.

Limitation of the Credit Union's Liability

The Business expressly agrees that the Credit Union will not be liable for any loss (however arising, including negligence), arising from or related to:

- The Business's failure to properly activate, integrate, or secure its Account.
- Fraudulent transactions processed through its payment gateway account.
- Disruption of the Credit Union services, systems, server, or web site by any means, including, without limitation, distributed denial of service ("DDoS") attacks, software viruses, Trojan horses, worms, time bombs, or any other technology.
- Actions or inactions by any third party, including, without limitation, a Business' service provider, payment processor, or other Credit Union.
- Unauthorized access to:
    - Data, Business data (including credit card numbers and other personally identifiable information), transaction data, or personal information belonging to the Credit Union, the Business or any third party.
    - The Services, or any system or program associated herewith.
    - The limitation of the functioning of any software, hardware, equipment, or service.

The Credit Union and the Business acknowledge and agree that the limitations of liability in this section are a bargained for allocation of risk and liability and agree to respect such allocation of risk and liability. Each party acknowledges and agrees that the other party would not offer the Services subject to this Agreement without the limitations of liability set forth in this section.

Intermediaries

The Credit Union may act on any communication and provide the Services using any payment system or intermediary organization it reasonably selects. The Credit Union's performance of the Services is subject to the rules and regulations of any such system or organization. The Credit Union may engage third parties to provide the Services. The Credit Union shall have no obligation to disclose arrangements with third parties to the Business or obtain the Business's consent thereto. The Business authorizes the transfer of information relating to the Business to agents of the Credit Union or the Business for use in connection with the Services or as required by law.

Credit Union's Responsibilities

The Credit Union will deliver to the Business, or otherwise provide access to, the Software and the Authorized Equipment.

The Credit Union will provide installation and training support as reasonably required for the Business's implementation of the Services. Any onsite installation or training support outside of King County, Washington, shall be on such terms and conditions as the parties agree, including reimbursement for the Credit Union's reasonable travel costs.

The Credit Union will provide maintenance and support for the Software as reasonably necessary to permit the Business's processing of Checks through the Services. Such maintenance and support shall include:

- Corrections, work arounds, and bug fixes.
- Such modifications, enhancements, and updates as the Credit Union elects to make generally available to businesses with or without additional license fees.
- Telephone support to the Business during the Credit Union's regular business hours.

The Credit Union will accept for deposit to the designated Account(s) digitized images of Checks that are transmitted to the Credit Union in compliance with this Agreement. Digitized images shall be deemed received by the Credit Union upon Successful Receipt of the transmission of such images that are complete, usable, and legible. If the digitized images are not complete, are not useable, or are not legible, the images may not be processed by the Credit Union or its agents, in which event the Business's deposit will be adjusted and notification will be provided. Final determination of image quality will be at the discretion of the Credit Union.

The Business's digitized images will be processed after Successful Receipt. If Successful Receipt occurs after 3:00 p.m. Pacific Time (PT) on a Business Day, processing will not occur until the next Business Day. The Credit Union will use commercially reasonable efforts to present Electronic Checks and Substitute Checks for collection.

In the event the Services are temporarily unavailable, there are other options for deposit. In-person branch deposit, ATM deposit, Night depository deposit, or the Business may also send items for deposit to the Credit Union via regular mail to **ATTN: Salal Credit Union, PO Box 7492, Carol Stream, IL 60197-7492**.

If a Payor Financial Institution returns an item to the Credit Union unpaid, the Credit Union will charge the Business Account for such returned item, and may either:

- Return the item to the Business or;

- Re-present the item to the Payor Financial Institution before returning it to the Business. Items may be returned as Image Exchange Items (as defined in Regulation CC), rather than IRDs, as agreed by the parties.

If a Payor Financial Institution or other third party makes a claim against the Credit Union or seeks a re-credit with respect to any Electronic Check, the Credit Union may provisionally freeze or hold aside a like amount in the Business Account pending investigation and resolution of the claim.

The Credit Union may suspend immediately the Services or the processing of any Check or corresponding Electronic Check if the Credit Union has reason to believe that there has been a breach in the security of the Services, fraud involving the Business's Account or such Check, or any uncertainty as to the authorization or accuracy of Electronic Checks. The Credit Union reserves the right at any time to process Electronic Checks on a collection basis.

Business Responsibilities

The Business will maintain an Account at the Credit Union for the receipt of deposits of digitized images of Checks, in accordance with applicable *Business Membership & Account Agreement*.

The Business will install the Software and Authorized Equipment in accordance with the RDC Documentation and will install and implement any changes and upgrades to the Software as the Credit Union may require, within 30 days of receipt of such change or upgrade, or within such shorter time frame as the Credit Union may reasonably require in the event such change or upgrade is necessary to comply with statutory or regulatory changes or developments, or to protect the integrity and security of the Services.

The Business shall use the Authorized Equipment to scan the Original Check, the result of which will be to create a digital image of the front and back of the Original Check, which has a legible payee, handwritten or typewritten dollar amount, numerical dollar amount, and MICR data, and which is in a format that will allow the Credit Union to create an Electronic Check or a Substitute Check.

The Business is responsible for ensuring the dollar amount of each Electronic Check is based on the legal written dollar amount from the Original Check.

The Business is responsible for verifying the accuracy of all MICR data captured by the Authorized Equipment by visually comparing the image in the Software to the Original Item. To ensure accuracy, the Business is responsible for re-scanning the Original Item or making any necessary edits within the Software.

The Business will ensure all Original Checks are endorsed with their name and a restrictive endorsement (such as "For Remote Deposit Only at Salal CU"), regardless of whether the RDC Service provides a virtual or electronic endorsement.

The Business will use the Authorized Equipment and the Software, including the entering, processing, and transmittal of items, in accordance with the RDC Documentation. The Business must limit the use of all Authorized Equipment to the processing of transactions with the Credit Union. The Business may not use the Authorized Equipment with any other Person or for any other purpose without the prior express written authorization of the Credit Union. The Business will ensure that the scanner will be located in a physically secure location. The Business will ensure the Authorized Equipment is clean and operating properly and will inspect and verify the quality of images and that the digitized images of Checks are legible for all posting and clearing purposes.

The Business will ensure that no financial institution (depositary, collecting, or payor), drawee, drawer, or endorser, with respect to a Check processed by the Business, will receive presentment or return of, or otherwise be charged for, the Check (including the Original Check or Substitute Check), corresponding Electronic Check, and/or other paper or electronic representation of the Check such that such person will be asked to make payment based on an item that it already paid. The Business will not deposit Checks more than once.

The Business will not use the Services to deposit the following:

- "Third-Party Checks" or Checks that are endorsed over to the Business.
- Checks drawn on the same account where the deposit is being made.
- Foreign Checks.
- Cash.
- Previously deposited items.
- Travelers Cheques.

The Business will take all commercially reasonable precautions to prevent the introduction of a computer virus, malicious code, or other defect that might disrupt the operations of the Authorized Equipment or the Software, including the installation, operation, and proper configuration of commercially reasonable anti-virus software. The Business will comply with all security procedures described in the RDC Documentation (including, but not limited to, the security guidelines that accompany the Agreement in Appendix A) and will not bypass, override, or disable any security mechanisms in the Authorized Equipment or Software. The Business is also responsible for regularly reviewing the security of their computers and networks to ensure these precautions are effective.

The Business will assign an Administrator on the enrollment form. The Business may change the Administrator at any time by contacting the Credit Union and signing a new enrollment form. The Administrator is responsible for adding, removing, and monitoring all users entitled to access the Services. This includes assigning access to the Services by assigning login credentials as applicable, assigning access to accounts, assigning dollar limits, ensuring adherence to the terms of this Agreement as well as the Business's internal controls and security procedures.

The Business is solely responsible for maintaining adequate security and control of all login credentials issued by the Administrator and will restrict access to login credentials as necessary. The Business will be responsible for training its employees in the use of the Services, and for supervising and auditing their use of the Services. This includes training for its employees and agents on the identification of fraudulent, counterfeit, altered, and forged Checks, and the proper safeguard and disposal of Checks as required by this Agreement.

The Business will retain each Check for a reasonable period of time, but in no event fewer than 15 days or greater than 60 days after such Check has been digitized and processed. The Business will promptly provide any retained Original Check (of if the Check is no longer in existence, a sufficient copy of the front and back of the Check) to the Credit Union as requested to aid in the clearing and collection process or to resolve claims by third parties with respect to any check.

The Business will use a commercially reasonable method approved by the Credit Union to destroy checks after the Business's retention period has expired

(e.g., a cross-cut shredder or a commercial shredding vendor).

While Checks are in their possession, the Business will take all reasonable measures to comply with industry standards for the security and safekeeping of all Checks prior to their destruction. Industry standards include, but are not limited to, use of locked storage and restricted access.

In the event of lost, mistaken, incomplete, or unusable Electronic Checks, or in the event of claims of fraud, alteration, counterfeit, or otherwise, the Business shall cooperate fully with the Credit Union in providing information.

It is strongly recommended that the Business establish an Incident Response Plan or procedures for notifying their customers and vendors if a security breach, theft, lost items, or other security deficit at the Business's place of business or of the Business's computer systems has resulted in the accidental or intentional compromise of their confidential account information.

The Credit Union may, from time to time, request that the Business provide financial information including, but not limited to, tax returns for review. Failure to provide the requested information may be cause for the termination of the Services.

In the event that the file containing the digitized images is unable to be transferred to the Credit Union, the Business should use an alternate means to make the deposit (same means as existed prior to the commencement of the Services)

If an item is "dishonored" (charged back), the Business will receive an image of the Original Check or a Substitute Check as the charged back item.

The Business agrees to promptly contact the Credit Union in the event they experience a security breach that may compromise confidential information.

The Business agrees to promptly return the Authorized Equipment to the Credit Union should the Services be terminated for any reason. If the Business does not promptly return the Authorized Equipment, the Business agrees to pay the Credit Union, on demand, the then-current replacement cost of the Authorized Equipment without any deduction for depreciation, wear and tear, or physical condition of the Authorized Equipment. The Business authorizes the Credit Union to charge the Account for such costs. The Credit Union may also continue to charge the Business all applicable fees until any remaining Authorized Equipment is returned.

User Roles

The Administrator is responsible for creating and deleting RDC User or RDC Admin User profiles and assigning access to enrolled Accounts. The Administrator cannot create, scan, or transmit Remote Deposit transactions via the Service.

- **RDC User** - creates and scans transactions but cannot approve transactions for transmission to the Credit Union.
- **RDC Admin User** - creates, scans, and approves transactions for transmission to the Credit Union.

Passwords and Sessions

- Users will be required to change their password the first time they access the Service.
- Passwords are encrypted and neither the Credit Union nor its Service Providers have access to this information.
- Users may change their password at any time through the "My Settings" function of the Service.
- Access to the Service will automatically be disabled after three (3) consecutive unsuccessful login attempts.
- The Administrator can re-set another user's password.
- Users are required to change their password every 90 days.
- Multiple users should not share a profile; each user should have their own login credentials.
- Sessions are automatically ended after 15 minutes of inactivity.

Physical Security

- Secure scanned items in a locked location, accessible only by authorized personnel, for a minimum of 15 days and a maximum of 60 days.
- Shred scanned items after the retention period using a commercially reasonable method such as a cross-cut shredder or a professional shredding service.
- Endorse all checks prior to scanning.

Injunctive Relief

Notwithstanding any dispute resolution procedures herein, the Business acknowledges that its violation of the sections of this Agreement entitled License and Confidential Information may cause irreparable injury to the Credit Union, and agrees that the Credit Union shall be entitled in the first instance, or at any other time, to seek temporary and preliminary injunctive relief in a court of competent jurisdiction, without the necessity of proving actual damages or posting a bond, to prevent such violation, and without being required to demonstrate that a money judgment would be inadequate as a remedy.

Appendix A: Security Guidelines

These guidelines are representative of a portion of the terms and conditions that pertain to the use of cash management services. They are intended to supplement the *Remote Deposit Capture Disclosure & Agreement*. Security guidelines must be fluid given the nature of financial fraud schemes, so the Credit Union in its sole discretion may revise these guidelines at any time. The Business's continued use of the Service(s) offered under this Agreement is consent by the Business to any new or revised Security Procedures.

General Security Guidelines

The Business and the Credit Union will comply with security procedure requirements established and/or amended by the Credit Union from time to time. Such security procedures are the for the purpose of evaluating the authenticity and protecting the confidentiality of Service requests ("Requests"). However, the Credit Union has no obligation to verify, review, edit, correct, amend, cancel, or reverse any such Requests, and will incur no liability with respect to the amount, accuracy, timeliness, or authorization of any such Request. If signature comparison is to be used as a part of such security procedures, the Credit Union will be deemed to have complied with that part of such security procedure if it compares the signature accompanying a Request (or a cancellation or amendment of a Request) received with the signature of an Authorized Signer and, on the basis of such comparison, believes the signature accompanying such file to be that of such Authorized Signer.

If a Request (or a cancellation or amendment of a Request) received by the Credit Union purports to have been transmitted or authorized by the Business, it will be deemed effective as the Business's Request even though the Request was not authorized by the Business, provided the Credit Union accepted the Request in good faith and acted in compliance with the security procedures referred to in the Agreement.

If the Business permits any other person to access any Service, the Credit Union will not be responsible or liable for such person's access, use, or misuse of the Services or accounts owned by the Business which were not authorized by the Business.

Business Responsibilities

The Business is solely and strictly responsible for:

- Determining, establishing, and maintaining internal procedures necessary to safeguard against unauthorized access to Services.
- Maintaining adequate security and control of any and all passwords, codes, security devices, and related instructions furnished by the Credit Union.
- Maintaining the confidentiality of security procedures.
- Restricting access to all passwords, codes, security devices, and related instructions to such employees and agents as may be reasonably necessary to use Services.
- Ensuring each employee or agent of the Business using Services is aware of and otherwise complies with all applicable provisions of the Agreement.
- Notifying the Credit Union immediately by written confirmation if the Business believes or suspects that any such information or instructions have been known or accessed by unauthorized persons or for unauthorized purposes.
- Securing the data residing on the server or other computer systems of the Business or a third party designated by the Business (e.g., a web-hosting company, cloud-based service, process, or other service provided), including, but not limited to, account numbers, security codes, and passwords.
- Ensuring their compliance with all applicable laws and regulations governing the Services.
- Installing and maintaining firewall, anti-virus, and anti-spyware software on their computers and networks.
- Establishing an incident response plan and procedures for notifying their users, customers, or vendors if any of their information was compromised due to a breach in security.

General Security Guidelines for Web-Based Services

Certain Services are available on the internet.

The Business is solely responsible for maintaining computer equipment in good working order, with the necessary compatibility and format to interface with all systems, including, without limitation, the ability to support security measures.

The Business shall install upgrades and other system enhancements within a reasonable time of being required to do so by the Credit Union.

There are a number of ways a criminal can gain access to Confidential Information via the internet. Here are a handful of threats every Business should be aware of. Please note: this list is not exhaustive; new methods of intrusion are developed every day.

- **Phishing/Spoofing** – Creating a fraudulent website or email disguised as a legitimate website or email designed to fool users into revealing Confidential Information to a hacker (i.e., usernames, passwords, credit card information).
- **Social Engineering** – A criminal tricks or deceives a person into divulging Confidential Information by posing as a trusted individual (i.e., a Credit Union employee).
- **Virus** – Malicious software that inserts itself into other programs or documents on computers and can be spread from computer to computer as documents and files are shared.
- **Worm** – Malicious software that spreads to computers on a shared network but does not require the sharing of documents or files to propagate.
- **Spyware** – Software that collects information about a user and then diverts that information to another person or company—often (but not always)

for use by a criminal or hacker. Often “piggybacks” onto a computer with the download of other, seemingly harmless software, sometimes without the knowledge of the user.

- **Trojan Horse** – A spyware program that purports to perform one function but is actually doing another, such as undermining the security settings or software on a computer, allowing a hacker to gain access.
- **Keylogger** – Spyware software designed to record every keystroke on an infected computer allowing a criminal access to passwords, credit card numbers, and other confidential information.
- **Password Cracking** – Attempting to discern a password through guessing or recovering stored data.

What follows are some general best practices for using Web-Based Services to assist in lessening the threat these schemes can pose to the Business and its users. Please consult with an internet technology expert for additional support or information.

- **Logging Off** – All Users should log off after every Service session to ensure the Service isn’t inadvertently left exposed to an unauthorized user. Online sessions will automatically end after periods of inactivity to protect Users who have left their computer unattended after logging in.
- **Public Networks** – The security of public computers (e.g., in a library, coffee shop, or internet café) cannot be assured. It is recommended that businesses refrain from accessing Services on a public computer or public wireless network.
- **Anti-Virus Software** – Businesses are required to utilize Anti-Virus Software from a reliable software provider and to routinely scan their computer(s), server(s), and electronic media for viruses. It is imperative that Anti-Virus Software be kept updated as recommended by the software provider to protect against new or developing virus threats.
- **Anti-Spyware Software** – Businesses are strongly encouraged to utilize Anti-Spyware Software from a reliable software provider and to routinely scan their computer(s), server(s), and electronic media for spyware. Spyware and viruses are not the same and Anti-Virus software may not be sufficient to protect against spyware.
- **Firewalls** – Software and/or hardware designed to protect computers and their contents by controlling the incoming and outgoing traffic on the network. When properly installed and maintained, it protects a computer against threats from the public Internet.
- **Security Updates and Patches** – From time to time, vulnerabilities are discovered in programs installed and/or running on a computer that may be exploited by criminals to gain unauthorized access to computers. Software publishers will release updates (or “patches”) to correct these weaknesses. THE BUSINESS IS REQUIRED TO KEEP COMPUTER OPERATING SYSTEM AND BROWSERS FULLY “PATCHED” FOR CRITICAL SECURITY ISSUES.
- **Electronic Communication** – Unencrypted email, fax, voice mail, text message, or other electronic communication methods are inherently unsecure and should not be used to communicate confidential information, passwords, account numbers, etc. Secure email programs can be utilized to encrypt data contained in these communications.
- **Password Protection** – Maintaining a secure, difficult to guess password is essential to ensuring security. Change passwords regularly and use a combination of alpha-numeric and special characters. Additional password guidelines are provided below.

Following these procedures cannot guarantee security but will significantly lessen exposure.

Passwords and Access Credentials Guidelines

By signing the *Remote Deposit Capture Enrollment* form, the Business agrees that its users will not share or make available their passwords or other means of access to Services or Accounts to any unauthorized individuals.

The Business assumes responsibility for all transactions and entries that are authorized via the Service, even those submitted by unauthorized individuals with whom passwords have been shared.

If the Business has reason to believe that a password belonging to its user has been compromised, lost, or stolen, or that an unauthorized individual has or may attempt to use the Service, the Business must notify the Credit Union immediately via secured email correspondence or by calling **206.298.9398** or **800.562.5515 ext. 8913**.

IF USERS DISCLOSE PASSWORDS TO ANYONE AND/OR IF USERS ALLOW SOMEONE ELSE TO USE THEIR PASSWORD TO ACCESS THE SERVICE(S), THE BUSINESS HAS AUTHORIZED THEM TO ACT ON ITS BEHALF AND THE BUSINESS WILL BE RESPONSIBLE FOR ANY USE OF THE SERVICE BY THEM.

Because a password is used to access account information and submit transactions, users should treat it as they would any other sensitive personal data:

- Carefully select a password that is hard to guess.
- Do not use words based on name, address, or other personal information.
- Special characters may be used to increase security.
- Do NOT use dictionary words.
- Keep all passwords safe.
- Memorize passwords and do NOT write them down.
- Change passwords regularly.
- Change passwords immediately if it is suspected that passwords have been compromised.

NEITHER THE CREDIT UNION NOR ITS SERVICE PROVIDERS WILL CONTACT A USER VIA TELEPHONE OR EMAIL REQUESTING THEIR PASSWORD. IF THIS HAPPENS, CONTACT THE CREDIT UNION IMMEDIATELY.

FAILURE TO FOLLOW THE ABOVE GUIDELINES MAY RESULT IN TERMINATION OF THE SERVICE.

In addition to the security features described above, there may be other security-related notices posted on the Credit Union’s website or the Service from time to time. It is the Business’ responsibility to read and follow all security notices.