Family First Credit Union
Remote Deposit Capture Policy

General Policy Statement
Remote Deposit Capture (RDC), a deposit transaction delivery system, allows Family First Credit Union to receive digital information from deposit documents captured at remote locations (i.e., the Credit Union's branches, ATMs, etc.) and on mobile devices. While RDC can decrease processing costs, support new and existing banking products, and improve members' access to their deposits, it introduces additional risks to those typically inherent in traditional deposit delivery systems.

The Credit Union will follow regulatory guidance addressing the necessary elements of an RDC risk management process in an electronic environment, focusing on RDC deployed at a member's location. This guidance is also applicable to the Credit Union's internal deployment and other forms of electronic deposit delivery systems (e.g., mobile banking and automated clearing house (ACH) check conversions).

Guidelines

PLANNING
Strategic Plan
The Credit Union will ensure that RDC is compatible with its business plan and strategies. The Credit Union will ensure its Strategic Plan demonstrates management has assessed the risks and documented the Credit Union's program to mitigate them, as well as the Credit Union's capability to provide the service.

Investments
The Strategic Plan will reflect any significant investment in information technology (IT) linking them to business-line goals and objectives.

Third Parties
The use of any third party service provider will be addressed in the Strategic Plan and will be tied to the Credit Union's Vendor Due Diligence policy.

Board Responsibilities
Unless otherwise delegated to management, the Board will approve the plans and expenditures related to RDC systems and services. The Board will also review periodic performance and risk management reports in the implementation and ongoing operation of RDC systems and services.

Management Responsibilities
Credit Union management will ensure it understands the return on investment and that it has the ability to manage the risks inherent in RDC. Management bears the responsibility for the safe and sound operation of RDC products and services, but may involve the following parties in the risk assessment, implementation or ongoing operations:

- IT and information security staff.
- Deposit operations staff.
- Staff responsible for business continuity planning and implementation.
- Audit and compliance staff (including BSA/AML).
- Accounting and legal staff.
- Third party vendors.

Risk Assessment
The Credit Union will perform a risk assessment regarding the risks associated with the RDC service and systems. This assessment will be conducted prior to implementation and will be reviewed on a periodic basis.

Legal and Compliance Risks
The Credit Union's management will identify and assess exposure to the various legal and compliance risks related to RDC. For each clearing method, the Credit Union will consider applicable legal and regulatory requirements (such as timeframes for handling returned items and funds availability).

- Warranties and liabilities associated with sending a check, in either electronic or paper form, to another institution for collection or presentment under the Check Clearing for the 21st Century Act (Check 21 Act), Regulation CC, Regulation J, applicable state laws (Uniform Commercial Code).

- Responsibilities with respect to the check as agreed to between the participating institutions by contract or clearinghouse rules.

- ACH transaction rules of the National Automated Clearinghouse Association (NACHA) and Regulation E.

- Issues associated with the laws and regulations of the Bank Secrecy Act, such as the exposure to the risk of money laundering or other suspicious activity, especially related to transactions performed by members deemed to be "high risk" under the Credit Union's member due diligence program, which is outlined in the Credit Union's Bank Secrecy Act policy.

- Requirements to perform a check of the Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list for all transactions performed through the RDC system.

Operational Risks
Operational risk is the risk of incurring a financial loss due to human or technical errors and fraud. The Credit Union will ensure that controls are in place to mitigate these risks, including physical and logical access controls over RDC systems, original deposit items at member locations, electronic files, and retained nonpublic personal information of members.

Effect on Existing Risks and Mitigating Controls
The Credit Union will carefully assess how RDC affects existing risks and mitigating controls. For example, for the various technological options, the risks associated with how and where nonpublic personal information is captured, transmitted, retained, and destroyed will be assessed. The Credit Union will consider the confidentiality, integrity, and availability of data afforded by its IT systems and by the systems used by the Credit Union's service providers and RDC users.

Scope and Complexity
The scope and complexity of the risk identification and assessment process will vary depending on the scope of RDC implementation and exposures faced by the Credit Union. For example, implementing RDC in the Credit Union's backroom operations may present less risk and complexity than deploying RDC at remote locations, such as members' business premises or homes, or on mobile devices, where the capture process is outside the direct control of the Credit Union. These risks can be unique to each member's location, access devices, RDC processing technology, and information security systems.

Document Management Procedures
In the typical RDC process, original deposit items are not submitted to the Credit Union but are retained by the member or the member's service provider. The Credit Union will require appropriate document management procedures to be implemented by the member in order to ensure the safety and integrity of deposited items from the time of receipt until the time of destruction or other voiding. These strategies will be employed in an effort to mitigate the following risks:

- Faulty equipment, inadequate procedures, or inadequate training of members and their employees can lead to inappropriate document processing, poor image quality, and inaccurate electronic data.

- Ineffective controls at the member location may lead to the intentional or unintentional alteration of deposit item information, resubmission of an electronic file, or re-deposit of physical items.

- Inadequate separation of duties at a member location can afford an individual end-to-end access to the RDC process and the ability to alter logical and physical information without detection.

Technology-Related Risks
Depending on the type of RDC system implemented, information security risks may extend to the Credit Union's own internal networks and networks of its service providers. These technology-related operational risks include failure to maintain compatible and integrated IT systems between the Credit Union, service providers, and the member. For example, a member or service provider may modify RDC-associated software or hardware or fail to update or patch an associated operating system in a timely manner. There also may be risks related to Web application vulnerabilities, authentication of a member to the RDC system, and encryption used at any point in the process.

Multi-Factor Authentication
The Credit Union will utilize multi-factor authentication to verify members utilizing its systems for RDC services (as well as all of the Credit Union's remote banking services) in order to mitigate the risks associated with fraud.

Fraud Detection
Duplicate presentment of checks and images at the Credit Union or another depository institution represents both a business process and a fraud risk. Check alteration, including making unwarranted changes to the Magnetic Ink Character Recognition (MICR) line on the image of scanned items, is difficult to detect when deposited items are received through RDC and are not inspected by a qualified person. Similarly, forged or missing endorsements, which may be detected in person, may be less easily detected in an RDC environment. Certain check security features may be lost or the physical alteration of a deposited check – such as by "washing" or other alteration techniques – may be obscured in imaging or electronic conversion processes. Counterfeit items may be similarly difficult to detect.

Securing Member Information
The Credit Union will assess the risks to the security and confidentiality of its members' nonpublic personal information. The Credit Union will adjust its information security programs in light of any relevant changes in technology, the sensitivity of member information, internal or external threats to information, and its own changing business arrangements.

MITIGATION AND CONTROLS

The Credit Union will employ the following risk management mitigation strategies and controls.

Member Due Diligence and Suitability

Given the risks associated with RDC, the Credit Union will reduce and control some of these risks by limiting the availability of this system to those determined to be "low risk" under its member due diligence program, which is outlined in the Credit Union's Bank Secrecy Act policy.

Suitability Review

For new and existing members, a suitability review will involve consideration of the member's business activities and risk management processes, geographic location, and member base. The depth of such review will be equal to the level of risk. When the level of risk warrants, Credit Union staff will visit the member's physical location as part of the suitability review. During these visits, the Credit Union will evaluate management, operational controls, and risk management practices, staffing and the need for training and ongoing support, and the IT infrastructure. Additionally, the Credit Union will review available reports of independent audits performed at the member location related to IT, RDC and associated operational processes.

Vendor Due Diligence and Suitability

All service providers used by the Credit Union for RDC services will be selected and monitored pursuant to the Credit Union's Vendor Due Diligence policy.

Contracts and Agreements

The Credit Union will consult with its legal counsel to develop and review its contracts and agreements with other financial institutions that accept checks in the form of electronic files, third-party service providers, and members that participate in the RDC process. RDC agreements should establish the control requirements identified during the risk assessment process and the consequences of noncompliance. Specific contract provisions for consideration include the following:

- Roles and responsibilities of the parties, including those related to the sale or lease of equipment and software needed for RDC at the member location if provided by the Credit Union;
- Handling and record retention procedures for the information in RDC, including physical and logical security expectations for access, transmission, storage, and disposal of deposit items containing nonpublic personal information;
- Types of items that may be transmitted;
- Processes and procedures that the member must follow, including those related to image quality;
- Imaged documents (or original documents, if available) RDC members must provide to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes;
- Periodic audits of the RDC process, including the IT infrastructure;
- Performance standards for the Credit Union and the member;
- Allocation of liability, warranties, indemnification, and dispute resolution;
- Funds availability, collateral, and collected funds requirements;

- Governing laws, regulations, and rules (such as cut-off times and the specification of how the member will know the Credit Union has accepted the deposit);
- Authority of the Credit Union to mandate specific internal controls at the member's locations, audit member operations, or request additional member information; and
- Authority of the Credit Union to terminate the RDC relationship.

Business Continuity

Credit Union management will ensure the Credit Union's ability to recover and resume RDC operations to meet member service requirements when an unexpected disruption occurs. The Credit Union's business continuity plan will address RDC systems and business processes, and the testing activities will assess whether restoration of systems and processes meets recovery objectives and time frames. To the extent possible, contingency plan development and testing will be coordinated with members using RDC.

Restrictive Endorsement

In order to mitigate losses in the case of fraud, the Credit Union will require the member depositing a check via RDC to include an endorsement similar to "**for mobile deposit only at Family First Credit Union (FFCU)**." This restrictive endorsement will not allow another depositary bank/credit union from making an indemnity claim if the original (paper) check it accepted bore this type of restrictive endorsement and inconsistent with the means of deposit. The Credit Union understands that without the restrictive indorsement, the Credit Union will indemnify the depositary bank/credit union that accepts the original (paper) check for deposit for losses incurred by the depositary bank/credit union if the loss is due to the check having already been paid.

Other Mitigation and Control Considerations

Management will implement, as appropriate, other controls that mitigate the operational risks of RDC, including those related to item processing. These controls will be designed and implemented to ensure the security and integrity of members' nonpublic personal information throughout the transmission flow and while in storage. Examples of such controls are as follows:

- Separation of duties or other compensating controls at both the Credit Union and the member location can mitigate the risk of one person having responsibility for end-to-end RDC processing.
- Strong change control processes coordinated between the Credit Union and the member can help to ensure synchronized RDC platforms, operating systems and applications, and business processes.
- To reduce the risk of items being processed more than once, deposit items can be endorsed, or otherwise noted as already processed.

- When insurance coverage is available and cost effective, the Credit Union may be able to mitigate risk further.

MEASURING AND MONITORING

For the effective oversight of RDC activities, the Credit Union will develop and implement risk measuring and monitoring systems. The Credit Union will ensure that members using RDC have implemented operational and risk monitoring processes that are appropriate to their respective choice of technology.

Key Operational Performance Metrics

Credit Union management will establish key operational performance metrics that support accurate and timely monitoring of risk within RDC processes. This information will be used to set operational benchmarks and standards, as well as to develop reports for monitoring results against the standards.

Reviewing Reports

Credit Union management will regularly review the reports and periodically conducting reviews and operational risk assessments. This will help ensure that the monitoring and reporting process accurately reflects current policies and procedures and sound practices. A variety of reports can facilitate management oversight of RDC operations, member compliance with agreements or contracts, and instances of questionable activity. Reports will address point-in-time activities as well as trends for individual members, groups of members with similar characteristics, and for the RDC product as a whole.

- Reports on duplicate entries (file and/or item recognition and interception) and violations of deposit thresholds may help monitor for unauthorized activities.
- Velocity metrics such as file size and number of records, transaction dollar value and volume, and return item dollar value and volume also assist in monitoring for fraudulent activity and capacity utilization.
- Reporting on reject items and corrections, and Courtesy Amount Recognition (CAR)/Legal Amount Recognition (LAR)/Intelligent Character Recognition (ICR) adjustments support monitoring of operational efficiency.