RED CROWN
CREDIT UNION

TECHNOLOGY COMMITTEE MEETING

August 17, 2018 – 11:30 AM

Red Crown Board Room – Southtown

RED CROWN CREDIT UNION

Technology Committee Meeting

Agenda

August 17, 2018 **Southtown Board Room**

1.	IT Report	Pgs 3	S. Richardson
2.	Merchant Capture Review	Pgs 4-7	C.J. Parker
3.	Red Flag Report	Pgs 8-10	C.J. Parker
4.	Sec. XIII - Information Security - Review	Pgs 11-42	J. Thornton

To: **Red Crown Technology Committee**

From: **Steve Richardson, Digital KeepSafe LLC**

Date: **8-17-2018**

Subject: **Technology Committee Report**

PC Refresh

- i7 Computers with Windows 10 Pro
- 50% completed
- What to do with i3 Computers
- Wipe HD
- Restore to factory settings with Windows 7 pro
- Keep newest for backups
- Employee purchase? How much

Personal Teller Machines (PTM's)

- ***This project is on hold pending more information from Finastra.***

Advance Alarms

- Project Lead - CJ Parker
- All branches completed except for Claremore
- Added Alarms and door fobs to emergency generator at Mayes County
- Claremore

Firewall F380

- Installed GEO Coding by country vs having to add specific IP Addresses.
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Includes VoIP Support (future phone system)

30 AMP UPS Battery Backup

- Had Electrician install new 30 amp circuit for UPS Battery Backup
- Replaces two older and smaller units.
- Part of our Server Rack clean up.

REMOTE DEPOSIT CAPTURE
REVIEW

August 2018

Remote Deposit Capture (RDC) is a process that makes depositing checks convenient for members who are unable to make it to the credit union on a daily basis. Annual reviews are conducted to ensure that proper procedures are being followed. This includes computer security and storage/destruction of checks. See below for the review on each account:

Member: MS Moser & Company CPA PC

Review Date : July 2018

Reviewed by: CJ Parker

Date account opened: April 26, 1991 RDC start date: October 1, 2010

1. Is RDC scanner in a location that cannot be seen by customers? ***Yes***
2. Are checks being stored in a secured area? ***Yes***
3. Are scanned checks being stored for 90 days per agreement? ***Yes***
4. How are checks over 90 days being destroyed? ***Member uses American Document Shredding.***
5. Are scanned checks encrypted before transmission? ***Yes***
6. Are virus/spyware scans conducted on a routine basis? ***Yes***
7. Does member have a secured system, ie: firewall? ***Yes***
8. Have there been any breaches, fraud or theft? ***No***
9. Is password to computer system in plain site? ***No***
10. Are there any changes to the RDC agreement? (additions/deletions) ***No***

11. Is the account in good standing? ***Yes***

12. Is the account handled in a positive manner? ***Yes.***
Any return items or negative balances? ***No. Member handles account as agreed.***

13. If member has loans, are they paid in a timely manner? ***N/A***

14. Was the review positive? If not, explain. ***Yes***

15. Was a review of the account history conducted? ***Yes. A review was conducted on the account and there were no return items from the clients.***

16. Any suspicious activity occurring on the account? If so, explain. ***No***

Ms Moser plans on purchasing a new computer in the very near future. She has scaled back on her clientele and plans to scale back a little more.

Member: Waterstone Cleaners

Review Date: August 2018

Reviewed by: CJ Parker

Date account opened: August 12, 2005 RDC start date: November 1, 2007

1. Is RDC scanner in a location that cannot be seen by customers? ***Yes***

2. Are checks being stored in a secured area? ***Yes***

3. Are scanned checks being stored for 90 days per agreement? ***Yes***

4. How are checks over 90 days being destroyed? ***Members bring voided checks to Red Crown to be destroyed.***

5. Are scanned checks encrypted before transmission? ***Yes***

6. Are virus/spyware scans conducted on a routine basis? ***Yes***

7. Does member have a secured system, ie: firewall? ***Yes***

8. Have there been any breaches, fraud or theft? ***No***

9. Is password to computer system in plain site? ***No***

10. Are there any changes to the RDC agreement? (additions/deletions) ***No***

11. Is the account in good standing? ***Yes***

12. Is the account handled in a positive manner? ***Yes***
    Any return items or negative balances? ***Minimal return items on customers.***

13. If member has loans, are they paid in a timely manner? ***Yes***

14. Was the review positive? If not, explain. ***Yes***

15. Was a review of the account history conducted? ***Yes, 6 months. No return check items during this period.***

16. Any suspicious activity occurring on the account? If so, explain. ***No***

This account also is a DBA for DeHoney's Cleaners

Member: FRSteam Oklahoma LLC

Review Date: August 2018

Inspected by: CJ Parker

Date account opened: January 26, 2015 RDC start date: February 9, 2015

1. Is RDC scanner in a location that cannot be seen by customers? ***Yes***

2. Are checks being stored in a secured area? ***Yes***

3. Are scanned checks being stored for 90 days per agreement? ***Yes***

4. How are checks over 90 days being destroyed? ***Members bring voided checks to Red Crown to be destroyed***

5. Are scanned checks encrypted before transmission? ***Yes***

6. Are virus/spyware scans conducted on a routine basis? ***Yes***

7. Does member have a secured system, ie: firewall? ***Yes***

8. Have there been any breaches, fraud or theft? ***No***

9. Is password to computer system in plain site? ***No***

10. Are there any changes to the RDC agreement? (additions/deletions) ***No***

11. Is the account in good standing? ***Yes***

12. Is the account handled in a positive manner? ***Yes***
    Any return items or negative balances? ***Minimal return items on customers.***

13. If member has loans, are they paid in a timely manner? ***Yes***

14. Was the review positive? If not, explain. ***Yes***

15. Was a review of the account history conducted? ***Yes, 6 months. No return times during this time period.***

16. Any suspicious activity occurring on the account? If so, explain. ***No***

This business account is owned by Jeff and Shelly Waters who own Waterstone Cleaners.

Submitted by:
CJ Parker-Internal Auditor

RED CROWN FCU ANNUAL

RED FLAG-IDENTITY THEFT REPORT

Summary

The Identity Theft Prevention Program Policy has been in place since November 2008. Incidents related to identity theft /Red Flags are tracked to determine the effectiveness of the policies and procedures and to identify any training gaps in the program.

Training

Training is conducted annually for all staff and for new employees upon hire. Policy, procedures and examples of Red Flags/Identity Theft are presented during training. Staff training for 2018 was a Power Point presentation conducted by the Marketing Department May 2018.

1. **Account Compromise**-RC continues to see account compromises due to member's information being stolen either by computer intrusion, theft of checks, credit/debit cards and different other types of scams, i.e.; Lottery, sale of goods online, social media, romance scams to name a few. If a member's account is compromised, they are advised to file a police report and when applicable, complete necessary affidavits. Members are advised to close out the compromised account and to submit a "fraud alert" on their credit through the credit bureau and to obtain a free credit report at annualcreditreport.com to see if there has been any suspicious activity or inquiries.

2. **Address Discrepancies**-An address discrepancy is determined if a potential member's address does not match what is on their driver's license/ID or a credit report reflects a substantial difference. New account/loans are reviewed to ensure the information obtained is in compliance with BSA account opening procedures. If a file is missing required documentation, the person that opened the account/loan is responsible for getting the missing information. All information must be substantiated.

3. **Credit Bureau Alerts**-In the event a credit freeze, fraud alert, or active duty alert appears on a credit report; staff will review the alert, call and verify the phone number that is on the credit report and verify with the applicant/member the reasoning for the alert. If applicant/member cannot answer the questions in regards to the alert, staff will notify Internal Auditor. Findings will be noted on the member's account.

4. **Credit/Debit Card**-All of Red Crown's credit and debit cards now have the EMV chip. Since the implantation, there has been a shift on how fraud is conducted. Most fraud is "card not present" (online/phone purchases) If an EMV card is compromised, it's usually due to cards being stolen or cloned. Skimmers are also a factor at ATMs and gas pumps.

5. **Fraudulent Phone Caller**-Occasionally Red Crown will receive a suspicious phone call on a member's account. If this should occur, staff will notify Internal Auditor and they will investigate and monitor the account. Notes are put on the affected account and emails are sent to staff.

6. **Lending**-Direct and Indirect Lending-Red Crown may receive applications from members or dealers that warrant further research. The Loan Officer, Indirect Lending Officer or I/L Assistant reviews the applications in questions and will contact the Internal Auditor for further research. If the application does not fit Red Crown's criteria, the application is sent back to the dealer or L/O will contact member to obtain additional information. If requested information is not presented, application is cancelled or denied.

7. **Online Account Opening/ID Theft/Mobile Deposits**-Since the implementation of U-Open and mobile deposits, Red Crown has seen possible fraudulent activity. Red Crown currently has designated staff reviewing online new accounts and mobile deposits to check for suspicious activity.

8. **Wires**-Red Crown Accounting Department handles all incoming/outgoing wires. Policies and procedures are in place to protect the member and credit union from fraud. Staff will notify Internal Auditor if they should encounter possible fraudulent activity.

Report of Incidents:

Summary of Incidents Related to Identity Theft/Red Flag Reports in 2018	Number of Incidents	Loss Yes/No
Account Compromise	2	No
Address Discrepancies	57	No
Credit Bureau Alerts	8	No
Credit Card/Debit Card	CC 2 DC 157	Yes
Fraudulent phone caller (posing as our member)	1	No
Lending-Fraudulent Application/Documents	1	No
Mobile Deposits	23	Yes, three
Online Account opening-ID Theft	11	Yes, one
Wires	0	N/A
Totals		

Red Crown receives and sends out fraud warnings from several agencies, i.e.; COCHA, CO-OP, CrimeDex, FBI, IAFCI, Infragard, and MAFIA. Contact with these agencies has proven to be invaluable in preventing possible fraud.

Red Crown staff is required to stay alert and report any potential fraud/red flags to their supervisor and Internal Auditor.

Submitted by: CJ Parker-Internal Auditor/Compliance/BSA Officer

SECTION XIII

INFORMATION SECURITY

Reviewed: ~~**September 2017**~~ **August 2018**
Approved: ~~**September 21, 2017**~~ **August 23, 2018**

Table of Contents

Page

Part 1 - Financial Privacy

Financial Privacy Statement 1
Information We Disclose 1
How We Protect Member Information 1
Risk Assessment 2
Financial Privacy Act 2
Notification Requirements 2
Grand Jury Subpoena 2
Training and Compliance 3
Record Retention 3

Part 2 – Member Information Security Program

Purpose 3
Confidentiality 3
Risk Assessment 3-4
Strategy 4
Implementation 4-6
Monitoring and Updating 6-7
Response 7
Disaster Recovery 8
Training 8
Testing 8
Member Education 8

Part 3 – E-Commerce

Purpose 8-9
Electronic Commerce Activities Defined 9
Credit Union Website 9
Online Banking 9-10
Mobile Banking 10
Online Bill Payment 10-11
E-Statements 11
Email/Email Encryption/Electronic Signature 11-13
ATM/Debit Cards 13
ACH System 13

Remote Deposit Capture 13-14
Wire Transfers 14
Disaster Recovery 14
Communication Safeguards 15-16
Communications Network 16
Response Program 16
Summary 16

Part 4 – Red Flag

Red Flag Statement 17
Identity Theft Program 17-18
Safeguarding Consumer Information 18
Identifying Persons Who Open New Accounts 18
Third-Party Providers 18
Member Address Changes and Discrepancies 19
Training Employees 19
Educating Consumers 19
Internal Audit 19
Identity Theft / Incident Response Program 19-25

Attachments

Attachment A: Member Information Systems
Attachment B: IT Risk Assessment
Attachment C: Tech Usage Policy
Attachment D: Red Flag Product and Services Risk Assessment

Part 1 - Financial Privacy

Financial Privacy Statement

Red Crown Federal Credit Union is committed to making available financial products and services that will enable its members to meet their financial needs and goals. Protecting personal information and using it in a manner consistent with member expectations is a high priority. To ensure that members can rely upon the quality of products and services we make available, Red Crown Federal Credit Union stands behind the following privacy policy:

- Red Crown Federal Credit Union will collect only the personal information that is necessary to conduct our business. We collect this information about members from applications and other forms, from member transactions with us, member transactions with nonaffiliated third-parties and information we receive from consumer reporting agencies.
- Our members will always have access to their information. Members of Red Crown Federal Credit Union have the opportunity to review their information and make changes to ensure that our records are complete and accurate.
- Red Crown Federal Credit Union does not and will not sell or provide any member information to non-affiliated third parties including list services, telemarketing firms, or outside companies for independent use.

Information We Disclose

Red Crown Federal Credit Union provides account information to companies that perform services or functions for the Credit Union, allowing us to offer and provide complete financial products and services. We may disclose all or some of the information we collect to companies that perform marketing services on our behalf or other financial institutions with which we have joint marketing agreements. We may also disclose information we collect under other circumstances as permitted or required by law. These disclosures typically include information to process transactions on our members' behalf, to conduct the credit union operations, to follow member instructions as authorized, or to protect the security of our financial records.

How We Protect Member Information

Red Crown Federal Credit Union will comply with NCUA Rules and Regulations, Part 748, with regard to protecting our member's personal information. Red Crown Federal Credit Union will maintain strong security controls to ensure that member information in our files and computers is protected. We restrict access to member account and non-public information to those employees with a specific business purpose in using the information. Additionally, we maintain physical, electronic and procedural safeguards that comply with federal regulations and utilize leading industry practices to safeguard non-public personal information. Procedures for protecting member information are detailed in Red Crown's Member Information Security Program.

Risk Assessment

The Board of Directors recognizes there are internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information. Management is directed to reasonably identify all such risks to the credit union by using a process of monitoring, measuring and identifying all such risks for which the credit union must be prepared to control and mitigate. These assessments and the Member Information Security Program will be reviewed and updated not less than annually or whenever significant changes occur or new critical systems are introduced.

Management and the Board of Directors will be involved in decision-making processes to contain risks effectively. The Board will review and approve new products and delivery channels that may have significant impact on the credit union's protection of member information. Management will be expected to evaluate critically the design, operation, and oversight of product implementation plans, prepare such assessment reviews as is necessary and recommend changes to the Member Information Security Program as necessary.

Financial Privacy Act

Congress passed the Right to Financial Privacy Act (RFPA) to protect individuals' financial records from improper disclosure to federal agencies and officials. While Red Crown Federal Credit Union is legally obligated to respond to most subpoenas and other official requests for information and must file suspicious activity reports where appropriate, it will fully comply with the privacy law restrictions.

Red Crown Federal Credit Union will make every effort to protect member's financial privacy through compliance with the Right to Financial Privacy Act. Additionally, the credit union will provide appropriate member notification of subpoenas, summonses, written requests for information, and oral inquiries with respect to a member's financial information.

In order to release member information to a governmental agency or other party, the requesting party must provide a subpoena or other binding order or the written authorization of the member. Additionally, the requesting party must provide Red Crown Federal Credit Union with a certificate of compliance for each request of member information. Red Crown Federal Credit Union reserves the right to release such information, at its sole discretion, within the limits of the law.

Notification Requirements

Red Crown Federal Credit Union members normally will be notified by the credit union upon receipt of any subpoena or other written or oral order or request for information. However, the credit union will delay such member notification when instructed by a directive of the issuing court to delay notice with respect to federal subpoenas or other official inquiries.

Grand Jury Subpoenas

Red Crown Federal Credit Union will not provide notification to the member of certain grand jury subpoenas. Under no circumstances will a member named in a federal grand jury subpoena be

notified of the existence of the subpoena or the information disclosed pursuant to a federal grand jury subpoena.

Training and Compliance
The ~~VP/Sr. Vice-President of Operations~~ ***COO*** is responsible for initial and ongoing training of credit union employees of the requirements of the privacy policy. The credit union's compliance with the Right to Financial Privacy Act will be reviewed by the VP/Sr. Vice-President of Operations.

Record Retention
Red Crown Federal Credit Union will maintain a record and file of all requests for member financial information, including a copy of the request and the information released. The record may be made available to the member upon request, at the discretion of credit union management, unless prohibited.

All Other Credit Union Policies
It is the determination of the Board of Directors that the approved credit union policies and programs below shall be considered a part of this policy by reference:

- Member Information Program
- Red Flag Policy
- E-Commerce Policy

Part 2 – Member Information Security Program

Purpose
The lack of a comprehensive information security program, or the failure to adhere to the standards and practices described in the program, threatens the security, confidentiality and integrity of nonpublic member information. The Board of Directors and Management of Red Crown Federal Credit Union (RCFCU) have recognized this risk and have established the following policies and procedures to guard against threats and misuse of member information or member information systems. The Board will oversee the implementation and the maintenance of this program. Management will report to the Board on the status and effectiveness of the program at least annually.

Confidentiality
The contents of the information security program should be kept confidential and internal to RCFCU. The information contained in the program should be shared only with authorized employees and outside auditors or legal counsel when applicable. Disclosure of the contents of the program, whether intentional or accidental, could expose RCFCU to increased risk of security breaches, as specific information would help a potential intruder exploit known vulnerabilities in selected systems.

Risk Assessment

In the process of serving its members, RCFCU gathers nonpublic information. At times, in order to complete a transaction, it is necessary to disclose member information to a third party. Due diligence is exercised when selecting third-party processors and other service providers. Contracts with processors will require the processor to implement appropriate measures to meet the objectives of National Credit Union Administration (NCUA) guidelines for safeguarding member information. RCFCU requires Confidentiality Agreements with our service providers that have access to member information through their provision of services. These agreements require compliance to our privacy standards to ensure protection of our member information.

Member information comes in many forms, from electronic records to paper documents. As defined by the NCUA, member information means any records containing nonpublic personal information about a member, whether in paper, electronic, or other form that is maintained by or on behalf of the credit union. An inventory of member information systems and the sources and flow of member information has been documented in Attachment A.

Management has performed an Information Security Risk Assessment for RCFCU. Attachment B is a chart showing what the Board and Management consider to be potential threats to the security of its information. The chart also addresses potential damage, current control procedures, the adequacy of those procedures, and mitigation of the procedures. This information is reviewed annually and updated as necessary.

Strategy

An effective Member Information Security Program will ensure the security, confidentiality and integrity of nonpublic member information, and will include processes that mitigate risks of misuse of member information. There is a cost involved in implementing a program, and RCFCU must weigh the costs against the benefits of the program. We have made a substantial investment in information security that we believe protects our members' information. The program establishes and maintains appropriate standards relating to administrative, technical and physical safeguards for member records and information.

Our approach to member information security is in three parts: technical safeguards, physical safeguards, and our employees. These safeguards are intended to: insure the security and confidentiality of member records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any member or to the credit union. These three parts are described in more detail in the Implementation section below.

Implementation

Technical Safeguards

Our core data processor's security procedures include access controls on member information systems and controls to prevent its employees from providing member information to unauthorized individuals. Electronic data transmitted across communication lines is encrypted and/or password protected when it contains nonpublic member information. Risk management

of all outsourced technological services are controlled through service level agreements and contracts assuring vendors' security programs, their level of risk tolerance, their procedures for addressing risks and threats, and their procedures for notifying their clients should a breach of information security arise. Their assurance is documented through audit reviews including SOC 1 audits, as well as internal and third party audit reviews.

Internally, access to member information in electronic form is controlled by RCFCU's computer security procedures as described in the data-processing procedures manual. In brief, a user name and a password are required to sign on to the network. An additional user name and password are required to sign on to the data processing system where the most sensitive member information is stored. This password is required to be alpha-numeric and must be changed every 60 days. Employees are instructed not to share their passwords. The system access rights are assigned, controlled, and maintained by the VP/Sr. Vice-President of Operations. Workstations are located in areas not accessible to unauthorized persons during the day. Employees log off or lock their workstations when leaving their areas for extended periods of time. All workstations are either shut down or logged off at the end of each day to prevent access by unauthorized individuals. Other electronic equipment over which sensitive information is received will be located in restricted areas.

Currently, there is one laptop computer in use at the credit union. The laptop is assigned to the indirect lender. No remote access to RCFCU's network is allowed with the laptop. Information stored on the laptop has two levels of encryption which includes password protection. When not in use, the laptop will be stored in a secured area.

To protect our member's information from pretext calling or any unauthorized access by telephone, RCFCU will not give any account information by phone unless reasonably certain of the caller's identity and authority to the information. Caller ID is in place in all offices. This will alert the employee answering the phone if the call is coming from outside the area. Before giving any account information, it must be determined if the individual calling has proper authority to the information. This will be accomplished by using the member database system to ascertain what individuals have rights to the account. In order to verify identity, the caller must be able to give specific information about the account. If proper identification cannot be made, the account information will not be released.

Requests for address changes for member accounts must be validated. Acceptable forms of validity are written, faxed and mailed correspondence containing a member's signature, telephone call verification from the member if the code word is given, and email received through online banking secure messaging. Dual control procedures will be used for any activity involving a change in member address information or authorization.

Physical Safeguards

There are many physical documents received and stored by RCFCU that contain sensitive member information. These documents include but are not limited to: membership applications; loan applications; checks; credit reports; driver's licenses and other photo id's; and member correspondence. When possible, all member information will be stored in secured areas, such as one of the locking vaults. When member information is needed in an office or work area in order to complete a transaction, it will be safeguarded from access by unauthorized persons.

To protect confidentiality, documents containing member information will be placed in a drawer or folder if another member or other unauthorized person comes into the area. In addition, if an employee is leaving his or her workstation, all member information will be placed in a secured area.

Any discarded paperwork, disks, tapes, cassettes and all other media that contains member information will be destroyed in a manner that renders it unreadable. RCFCU utilizes a third-party service provider to handle destruction of documents from the main office. The destruction process includes shredding and then pulping. Certificates of destruction are provided by the vendor for all material processed by them. Crosscut shredders are utilized at the branch offices to destroy documents containing member information.

If it is necessary to allow a service technician into one of the restricted areas where member information is stored, an authorized employee will remain present to assure there is no improper activity that might compromise member information security. While we will make every effort to keep our member's information inaccessible to unauthorized persons, sensitive data received during the night (via fax or remote report printer) may be seen by cleaning contractor employees. Our privacy policy and information security program will be provided to service contractors and, when necessary, adherence to these standards deemed will be required in contractual arrangements.

Employees

Because all employees will come into contact with sensitive member information, new hires are considered very carefully with regard to integrity and background. Hiring standards include drug screening, credit report evaluation and criminal background checks. Former employers may be contacted for previous work performance and standards.

Upon employment, new hires will be given a copy of the Member Information Security program. In addition, all employees are required to read and sign a document outlining procedures for use of RCFCU technology (Attachment C).

Employees are an important part of information security. Training of our employees is critical, and RCFCU relies upon their judgment and confidentiality when dealing with member records. Employees should know, understand, and be held accountable for fulfilling their security responsibilities. In addition, employees should recognize, respond, and where appropriate, report any unauthorized or fraudulent attempt to obtain member information. Annual training will be provided to all employees.

When an employee is terminated, the ~~VP/Sr. Vice-President of Operations~~ ***COO*** and authorized IT personnel will immediately remove the employee's various system authorizations. Keys will be confiscated before the employee makes final departure. Applicable combinations and security codes that may be known by the terminated employee will be changed.

Monitoring and Updating

Information security procedures include monitoring systems and procedures to detect actual and attempted intrusions into our member database from outside sources. RCFCU utilizes an internal firewall, which is a device that monitors incoming and outgoing Internet activity and blocks unauthorized access into our private network. IT personnel work with IT consultants and/or the firewall manufacturers technical support personnel to assure the appropriate security levels are implemented. The core data-processing system generates daily reports that detail

member record changes. The Internal Auditor is responsible for the daily review of these reports.

RCFCU provides online banking to our members. Our core data processor provides firewall protection and monitoring. Member access requires a user name and password. Multifactor authentication has been implemented to comply with NCUA guidance regarding Internet banking security. Multifactor authentication has also been implemented on our audio response teller.

RCFCU utilizes software which includes virus and spyware protection, proactive threat protection, and network threat protection. Virus scans are performed automatically from a central management server which also provides for updates to all workstations. Monitoring software is used to gather data to take a proactive approach against hardware failures, potential network issues, and security related events.

The VP/Sr. Vice-President of Operations will monitor the handling of physical member records on an on-going basis. Procedures will also be included in the internal audit program to provide independent oversight.

Response

If a breach of security is suspected, the President/CEO will be contacted. If the President/CEO is not available, the, Controller/CFO or another member of senior management will be the contact person. Management will obtain guidance from our data processing provider and our IT consulting firm on containing and controlling the intrusion, while preserving records and other evidence.

A member of senior management will be notified immediately in the event of a security breach within the credit union, or if it is discovered that an employee has failed to follow information security procedures.

When an incident has occurred, management and the Board of Directors will assess the situation and the supervisory committee will be informed. The nature and extent of the breach and what member information has been accessed or misused will be identified. If member information has been compromised or an act of fraud has occurred, the NCUA and law enforcement agencies will promptly be notified. After the network has been secured the appropriate forms will be completed (e.g., SARs).

If RCFCU becomes aware of an incident of unauthorized access to sensitive information, a prompt investigation to determine the likelihood that the information has been, or will be, misused will be conducted. If a misuse of member information has occurred or is reasonably possible, any affected members will be notified as soon as possible.

Sensitive information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account.

The President/CEO, in coordination with the Vice-President of Marketing, shall be responsible for all communication with affected members as well as with the media and the public. RCFCU employees are instructed to direct inquiries from the public, including the news media, to the President/CEO.

Disaster Recovery
RCFCU has developed comprehensive Business Contingency procedures that include measures to protect member information if a system failure or natural disaster should occur. Procedures are detailed in RCFCU's Disaster Recovery Manual. Our core data processor disaster recovery plans are an integral part of the procedures and are also detailed in the plan document.

Training
Training with regard to RCFCU's privacy policy and information security program will be provided to new employees upon hire. An annual training meeting will be held for all employees. Additional meetings will be scheduled if changes are made to the policy and procedures, or if new regulations become effective. Training will include protection against information theft or fraud as well as procedures to report any actual or attempted breach.

Testing
Our core data processor's security program includes independent tests of its controls by a third party audit firm. The audit reports in addition to the third party audit reviews are made available to the RCFCU and are reviewed by the President/CEO, the CFO/Controller, and by the Credit Union's independent outside auditing firm.

Each department should perform ongoing assessments to ensure that credit union staff follows written procedures for member information security. The Internal Auditor provides an annual review of the Member Information Security Program and its internal information security controls.

Member Education
In an effort to educate our members on prevention of fraud and identity theft, RCFCU will provide printed information in its lobbies and as a statement stuffer or newsletter article at least annually. Additionally, information will be provided on our website and in periodic newsletters.

Part 3 – E-Commerce

Purpose

Red Crown Federal Credit Union recognizes the importance of electronic commerce (e-commerce) activities to its present day operations. The credit union is committed to using e-commerce activities in a cost effective manner that promotes accuracy, safety, security, and efficiency. These activities bring automation and efficiencies to traditional manual tasks and allow quicker access to information resulting in improved member service. This e-commerce policy communicates the strategic, operational, and risk management considerations that are presented by e-commerce and outlines the credit union's policy to manage these activities.

Electronic Commerce Activities Defined

Electronic commerce activities are defined as those electronic financial services delivered via electronic means including but not limited to the Internet or other electronic delivery vehicles. These services include the credit union's website, Online Banking, Online Bill Payment, Mobile Banking, UOpen, e-Statements, email, ATM/Debit cards, ACH transactions, Apple Pay**,** SamSung Pay, Android Pay, and electronic funds transfers. They also include business-to-business transactions where interaction is conducted electronically between the credit union and its business partners using the Internet as the communications network.

Credit Union Website

The credit union's website is hosted by a third-party. The Credit union's brand will be maintained throughout all web pages. Web pages will be reviewed periodically to ensure accuracy and quality. The credit union's internal auditor will perform a periodic review of the website and report to the Supervisory committee with related findings and recommendations

Security

Employee access to the Administrative Site is restricted to those employees authorized by the credit union, and is password protected. The Credit union will annually review employee user access privileges for appropriateness.

Privacy Policy

Red Crown's privacy policy can be accessed from the website. This policy will be reviewed and approved annually by the Board of Directors.

External Links

Our site may contain links to other web sites. Members are notified when leaving the credit union's website through a link. We are not responsible for the practices or the content of other web sites. However, we will monitor the addition of links and implement quality control measures to determine if the links are appropriate. All links will be reviewed on a regular basis.

Online Banking

In an effort to maintain competitive advantage and provide a high level of personalized service to our members, Red Crown offers account transaction services accessible through its core data processor. The credit union views this service as another delivery channel, not to supplant traditional member service, but to complement it.

Security

Red Crown's Internet transaction services are delivered through its core data processor. Red Crown will require the system vendor to maintain a high level of security in the form of:

- Multi-factor user authentication
- User options will include automatic time-out and require account holders to change the default password after initial log in
- ***TLS 2.0 (****Transport Layer Security)* ***is a method used to encrypt messages sent back and forth on a computer network between two devices. It is the current standard for message encryption and security. TLS Encryption has replaced SSL (Secure Socket Layer) encryption***.
- ~~Secure Sockets Layer (SSL), a minimum of 128 bit encryption~~
- Firewalls, filtering, and access control
- System vendor will receive a designated audit report.
- System vendor will hire an independent firm to routinely perform penetration and security testing

Online Banking Member Support

Only authorized employees will be allowed to process activation requests. The credit union's procedures will ensure that Online Banking services are removed in a timely manner for members that have requested de-activation or that have closed an account.

Mobile Banking

Mobile Banking is an extension of Online Banking. Red Crown's Mobile Banking offers account transaction services accessible through the use of mobile devices, which are used to access specifically, formatted web pages designed for mobile devices. Mobile Banking Security and member support is the same as Online Banking.

Remote Deposit Capture

Mobile Banking also features a 'Remote Deposit' application that is available for use with a select group of tablets and mobile phone vendors. This application is available to members when they meet specific requirements outlined in the procedures for this product. The "Remote Deposit" application will function with the same security and member support as Online Banking.

Mobile Payment Apps

These applications are available to members who want to use their applicable products to wirelessly pay for purchases. These applications will function with the same security and member support as Online Banking.

Online Bill Payment

As part of the convenience of online account transactions, Red Crown offers bill payment services accessible through its Online Banking service.

UOpen Banking

Electronic online application that is available through Red Crown's website. This product allows potential and existing members to open new membership accounts and apply for loans.

Verification of eligibility/membership is built into this product as outlined in the procedures. The UOpen application will adhere to the same security and member support as Online Banking.

Security

Bill Payment service is provided as part of our Online Banking product. The credit union recognizes the importance of the relationship between its core processing vendor and online service vendors due to security and interface requirements. The same security level will be required of this vendor, as outlined under Online Banking Security above.

Bill Payment Controls

The credit union's procedures will ensure that all accounts (e.g., remittance, expense, suspense, etc.) associated with online services are properly reconciled. The bill payment processor operates under what is commonly known as the "Guaranteed Funds Model." This model deters NSF situations as funds are debited from the member's account well in advance of the bill payment so the processor has good funds to transfer to the payee. The credit union maintains the ability at any time to turn on/off any member's bill payment privileges.

Bill Payment Processing

The bill payment processor verifies funds availability prior to authorizing bill payments, and then debits the member account on the date the payment is scheduled to be paid. The funds are debited from the member account and deposited in a settlement account at the Credit union. The bill payment vendor debits the Credit union settlement account rather than the member account. The member account is debited on the date they select the payment to be processed. Payments for vendors who only accept paper transactions need to be scheduled five business days in advance. Payments for vendors accepting electronic payments need to be scheduled two business days in advance.

Bill Payment Member Support

Red Crown will be the primary contact for member support. Only authorized employees will be allowed to process activation request. Bill payment services are removed in a timely manner for members that have requested de-activation or that have closed an account. The bill payment processor provides support to credit union staff.

E-Statements

Members' periodic account statements, along with any cancelled check images, are available over the Internet through an imaging service provided by a third-party imaging service. When a member requests e-statements, delivery of hard copies to the member is discontinued.

Security

Members who have requested e-Statements are required to set up a user ID and a password to gain access. Images are encrypted before being transmitted over the Internet. Our third-party imaging service provides additional security measures and is annually reviewed to ensure that these measures are sufficient.

E-Statement Member Support

Only authorized employees will be allowed to process activation requests. The credit union's procedures will ensure that e-statement access is removed in a timely manner for members that have requested de-activation or that have closed an account.

Email / Email Encryption / Electronic Signature

Email

Email is conducted with the use of an Internal Microsoft Exchange Server. Exchange is configured to send Inter office emails encrypted. All incoming and outgoing email is filtered via a two stage system. Incoming email is routed to Barracuda's cloud protection system where it is scanned for spam and malware. It is then forwarded to Red Crown's internal Barracuda Email Spam Firewall where it is filtered before being forwarded to the Exchange Server. Outgoing email is routed from the Exchange Server to the Internal Barracuda Email Spam Firewall where it is filtered then forwarded to Barracuda's Cloud Protection System where is scanned once more for spam and malware.

Email Encryption

While the Exchange server is configured to send interoffice email encrypted, Red Crown utilizes Barracuda's cloud protection services and the internal Barracuda Spam Firewall to add outgoing encryption to emails. The Spam Firewall is configured with predefined SOX, GLB, and HIPPA rules that filter outgoing email for rule violations. If an email rule is violated that email will automatically get encrypted and sent to Barracuda's Secure Message Center. Recipients then receive an email which provides a secure link to the Secure Message Center and the message displaying they have an encrypted message from Red Crown. Recipients must click the link where they are required to enter a password to access the secure message. Red Crown users can also send an encrypted message by clicking the "Encryption" button in their Outlook or by typing (Secure) in the subject line of the outgoing email.

Electronic Signature

An electronic signature is a paperless method used to authorize or approve documents which indicates that a person adopts or agrees to the meaning or content of the document.

Federal law (the federal E-Sign law) defines an electronic signature as: "an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."

The federal government authorized the use and acceptance of electronic signatures in The Electronic Signatures in Global and National Commerce Act (E-Sign).

Red Crown allows the use of electronic signatures as an acceptable alternative to an original signature for those documents requiring signature or acknowledgement and uses DocuSign as the electronic signature vender.

User's log in to DocuSign via an SSL encrypted connection where documents are uploaded for electronic signature processing. Once documents are tagged with the required needed

information, they are emailed to the recipients using an SSL encrypted delivery connection. Recipients are required to enter an access code provided verbally by the Document Processor/Sender. Once the recipient receives the email they must enter the access code in order to open the document. Once the required information has been completed it is emailed to the original sender where the document can be downloaded to a specified location, printed or retained in the original sender's profile.

Users are currently required to print a copy of the court-admissible, digitally signed and tamper sealed Certificate of Completion that contains a comprehensive digital audit trail of the completed documents.

Electronic signature through DocuSign provides full document encryption to ensure the confidentiality of data. Documents are stored in ISO 27001 and SSAE 16 data centers and are encrypted with AES-256 standard and uses 256-bit SSL document transmission.

ATM/Debit Cards

Red Crown utilizes TransFund as its Automated Teller Machine (ATM) and debit card processor. The credit union owns four ATM machines. Members have access to free transactions at hundreds of ATMs through TransFund's no surcharge network and the cooperative ATM Zone network.

Security

ATM card transactions require the use of a Personal Identification Number. Account and transaction data transmitted over the ATM network is encrypted. Account numbers are truncated on any printed transaction receipts. Member debit card transactions are monitored for suspicious activity by the third-party processor.

ATM/Debit Card Member Support

Only authorized employees are allowed access to the card system. When a member has applied and is approved for an ATM and/or debit card, a card is ordered through the vendor's system. Another staff member, who does not have access to the card ordering system, reviews a daily new accounts report to verify accuracy of the card information. TransFund mails the new card directly to the member. The Personal Identification Number is mailed separately to the member three days later. The credit union's procedures will ensure that ATM/Debit cards are de-activated in a timely manner for members that have requested de-activation, that have closed an account, or that have suspected fraudulent activity involving the card.

ACH System

Automated Clearing House (ACH) files are received and sent through the core data processing system. Only authorized employees are allowed access to the ACH functions. Reports are received and reviewed daily by authorized personnel. The credit union's procedures will ensure that all accounts associated with ACH processing are properly reconciled daily. The internal auditor conducts an annual audit of the ACH procedures.

Merchant Deposit Capture (MDC)
MDC is a deposit transaction delivery system which allows Red Crown to receive digital information from deposit documents captured at remote locations. These locations are the place of business for the Red Crown member.

MDC can decrease processing costs, support new and existing banking products, and improve member's access to their deposits. MDC does however introduce additional risks to those typically inherent in traditional deposit delivery systems.

Red Crown uses its core data processor for all merchant deposit capture processing. Once the merchant scans the check the image is sent securely to the vendor via a 128 bit SSL Internet connection.

Red Crown requires all merchant's using MDC to have a signed contract on file stating they will abide by the Merchant Capture Policy and all associated procedures.

Annual visits to the merchant's physical location are performed by the Credit Union's Compliance Officer to ensure member compliance of all appropriate policies and procedures.

Wire Transfers
Red Crown's wire transfer policy establishes the guidelines by which all incoming and outgoing wire transfers must follow. The wire transfer instruction form is completed when necessary by authorized employees and used for tracking and verification purposes. All wires must adhere to the following guidelines:

All member wires to domestic financial institutions are executed via FedLine. FedLine security settings require one person to create the wire and a second person to verify. The President/CEO is the system administrator for FedLine. The President/CEO does not have verify or send capabilities.

International wires and wires to transfer Red Crown funds between internal accounts are executed via a correspondent bank by the Controller/CFO or the President/CEO. These wires are verified via callback by the correspondent bank.

A wire log shall be maintained listing all pertinent details of the transaction including origination of funds such as account loan proceeds, cash, etc. All wires executed with cash shall be brought to the attention of the BSA officer.

The wire transfer form is filled out and a debit to the account is signed by the member for each wire. An exception is when an existing customer sends a fax request that is signed. Telephone wire transfers are acceptable only if the member initiating the wire has a prearranged agreement on file. Any wire over $3000 requires a call back to ensure verification of the caller.

Members who initiate wires on a reoccurring basis must have a prearranged wire transfer form on file. Wires are sent with collected funds only. Two forms of ID are required for all wires unless a signature is provided. All wires require OFAC verification. Red Crown Credit Union only accepts wire transfer requests from established customers.

Disaster Recovery

Red Crown's website, Online Banking, Online Bill Payment, Mobile Banking and e-statement reside on vendors' host data centers. These systems will remain in operation in the event of disaster impacting Red Crown. Because these services are data center/ Internet based solutions, the credit union has the ability to monitor the systems offsite. The ATM/Debit card and ACH

system files are processed online by the core data processor and would also remain in operation in the event of a disaster. Specific recovery procedures are detailed in the credit union's Disaster Recovery and Business Continuity Plan.

Communication Safeguards

It is the practice of the credit union to safeguard member data at all times, including the processing of e-commerce transactions. Information must be protected at both the sending and receiving ends of each transaction. To accomplish this, there are several levels of protection applied to e-commerce activities.

Encryption

Encrypting transactions provides security by ensuring that no portion of a transaction is readable except by the parties at each end of the transmission. This ensures that data can be transmitted securely without concern that another party could intercept all or part of the transaction. Encryption also makes certain that the transaction is not tampered with as it routes from point to point. Data is received exactly as it was sent.

Authentication

After a secure connection is established, the initiating party must prove their identity prior to conducting the transaction. This is typically handled with user IDs or account numbers along with password or PIN combinations. Additionally, encryption certificates are also employed to validate the authenticity of both servers and users. System administrators control system access by assigning users different levels of access for applications and data. These access levels are determined by senior management and are specific to each job function. This ensures that access to applications and specific types of transactions are only granted as job functions require.

Firewalls

A firewall is a device that stands between two networks and determines what information is allowed to pass between them. Because it analyzes all traffic passed in either direction, it can deny connections to services that have the potential to compromise our systems. RCFCU utilizes a firewall to block all unwanted Internet access ensuring the integrity of the internal network and its resources.

Network Traffic Rules and Restrictions

Intra-network traffic is subjected to distinct operating rules and restrictions. Relying upon a firewall and Internet best practices, no external traffic is allowed to access any internal device, unless the device initiated the communication. This strategy dramatically reduces the risk of any party gaining unauthorized access to a protected server.