RED CROWN
CREDIT UNION

TECHNOLOGY COMMITTEE MEETING

November 16, 2018 – 11:30 AM
Red Crown Board Room – Southtown

RED CROWN CREDIT UNION

Technology Committee Meeting

Agenda

November 16, 2018 **Southtown Board Room**

1.	IT Report	Pgs 3	S. Richardson
2.	Security Report	Pgs 4-5	C.J. Parker
3.	Policy Update – Sec. XIII –Information Security	Pgs 6-8	J. Thornton

To: **Red Crown Technology Committee**

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

Date: **11-16-2018**

Subject: **Technology Committee Report**

PC Refresh

- i7 Computers with Windows 10 Pro
- 90% completed

Phone System

- Cloud based solutions
- Narrowed vendors to two
- Mitel Cloud vs 8x8 Cloud
- Had Demo on both systems
- Following up with questions
- Important Features
    - Call Center Management
    - Texting and Chat
    - Integration with Polycom system for conference calling
    - Call recording and storage
    - Phone Options (physical - Softphone for PC - app for Smartphones)

Finastra Annual User Conference

- Scottsdale Arizona
- Deanne, Joyce, Steve will be attending

Red Crown FCU

Branch Security Report

November 2018

In accordance with Part 748 of NCUA Rules and Regulations, federally insured credit unions are required to institute a written security program. The program also requires the Security Officer to conduct an annual branch security review and report such findings

Red Crown currently has four (4) branches:

South Office- 5001 E 91st Tulsa
Midtown- 5321 E 41st ST Tulsa
BA Branch - 3101 W Kenosha Broken Arrow
Mayes - 19 N Rowe Pryor

***Claremore branch to open early 2019

Physical Security

- Alarm system and cameras have been upgraded at all branches. Branches are accessed using a keyless fob, with the exception of Midtown which key entry is used. All branches have hold up/panic buttons and maglocks. Testing is conducted in conjunction with our alarm company periodically to ensure all devices are working.
- Midtown has an off-duty police officer on Saturdays and during the Christmas holiday through the end of the year.
- Windows and exterior doors at all locations are secure and can be viewed by law enforcement from outside.
- Random inspections of the branches are conducted before opening to ensure all sensitive information is not left on desks or printers from the day before. All sensitive information must be locked up in cabinets, desks, or in the vault room.
- ATM's are checked periodically for skimming devices.

Findings: None

Cash Control

- ST, MT, MC, and BA offices are using cash recyclers. Cash drawers are in use at MC and MT for tellers who are not using the recyclers. Cash recyclers serve as a vault, records all serial numbers being deposited and withdrawn, thus eliminating the need for bait money, and detects counterfeit bills. Dual control is required for access to all recyclers, ATMs, and vaults.

Findings: None.

Robbery/ Security Training

- Robbery and security training are mandatory and is conducted annually for all staff and for new employees upon hire.

Opening/Closing

- Opening, closing, fire and severe weather procedures vary from branch to branch and are reviewed with staff.

Crime Trends:

- Bank robberies and casings in the Tulsa and surrounding areas have dropped considerably in the past year. Staff is alerted to any casings or robberies in the area and is advised to notify their supervisor and the security officer in the event they notice any suspicious activity or behavior.

Security Officer Training

- The Security Officer keeps up with training through seminars, webinars and memberships in several groups such as: MAFIA (Metro Area Fraud Investigators Association) and Infragard through the FBI.

Report submitted by: CJ Parker Internal Auditor/Security Officer

Date: November 19, 2018

To: Technology Committee

From: Management

Reference: Policy Section XIII – Information Security

In response to Hogan Taylor's recent Agreed Upon Procedures, Management is recommending the following changes to policy Section XIII – Information Security following this memo.

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~~ ***W***ires to transfer ***funds between*** Red Crown ***owned accounts*** ~~funds between internal accounts are executed via a correspondent bank~~ ***are authorized*** by the Controller/CFO or the President/CEO ***and executed by accounting staff***. ***Wires from FHLB to FedLine require a call back approval, per FHLB. Approval can be given by President/CEO, Controller/CFO, or COO.*** ~~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.~~ ***Exceptions include a faxed request that is signed (signature will be verified with existing records), secure messages within online banking, and a verifiable electronic signature with DocuSign which originated at Red Crown. Telephone wire transfers are accepted only if the member has a signed Wire Transfer Agreement on file. All telephone wire transfers are handled by the Accounting Department. Any telephone wire transfer over $10,000 requires a call back to ensure verification of the caller's identity.***

Members who initiate wires on a reoccurring basis ~~must~~ ***may*** have a ~~prearranged~~ Wire Transfer ***Agreement*** 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 ***members*** ~~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