2800. E-COMMERCE POLICY

TABLE OF CONTENTS

E-Commerce Policy

Resource One Credit Union's Board of Directors and management recognize their responsibility to protect member's financial safety from fraud and identity theft and the importance of electronic commerce (e-commerce) activities to its present day operations. Further, Resource One Credit Union considers the management and security of this electronic information to be of critical importance and is committed to enhancing member service through the use of many forms of e-commerce activities. The Credit Union is committed to using e-commerce activities in a cost-effective manner that safeguards member data and promotes accuracy, safety, security and efficiency.

E-commerce services must be:

- Monitored for member activity and availability.
- Measured for member satisfaction.
- Evaluated for the financial impact these offerings have on the organization.
- Monitored for safety and security of member information.

These standards shall ensure the e-commerce services provided by Resource One are implemented and maintained with the aforementioned factors in mind. Further it is to be used as both a guideline and an overview in the management of the Credit Union's electronic services.

Resource One Credit Union will implement comprehensive policies, standards, and procedures that will prescribe assessing existing risks associated with each e-commerce activity before implementation, developing ways to manage and control the existing risks, and procedures for monitoring third party outsourcing arrangements to ensure compliance

with Credit Union policies and procedures. Compliance with these standards will be ensured through periodic audits conducted by internal audit or an independent third party.

ORGANIZATIONAL RESPONSIBILITY

Senior management is responsible for ensuring that proper risk management steps are taken when evaluating and monitoring e-commerce services. Senior management's objective is to assure that long and short-term e-commerce resources and strategies are formulated and approved, sufficient to support the Credit Union's overall business objectives and strategies. Senior management will ensure the risk management process is maintained through the:

- Performance of risk assessments.
- Performance of due diligence evaluations.
- Evaluation of contracts.
- Implementation of an oversight program.

Senior management will also:

- Respond to problems that have escalated beyond the primary responsibility.
- Document periodic reviews/discussions of e-commerce activities.
- Provide periodic updates to the Technology Committee on e-commerce products and services, security activities, problems and their solutions, current and historical usage, recommended changes and improvements and any other significant e-commerce issues.

E-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, email, telephone access system, online bill payment and Internet and Mobile Banking services. 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.

Specific examples of e-commerce activities include:

- Internet/Consumer website services:
  - Credit Union website
  - Email inquiries and responses
  - Publishing of general information on the Credit Union website
  - File transfers of member information for direct mail projects or statement generation
  - Online membership application
  - Online loan application
  - Apply for loans or other Credit Union services
- Internet Banking
  - View account balances
  - View share or loan transaction history
  - Transfer funds between accounts at the Credit Union
  - Transfer funds to other Credit Union member accounts (pre-authorization required)
  - Transfer funds to parties outside the Credit Union using Online Bill Pay
  - Apply for loans or other Credit Union services
  - Check loan information and make loan payments
  - Receive monthly statements electronically with e-statements
  - Request a check withdrawal from a share or loan
  - Request a stop payment on a check
  - Instant deposit
  - View credit card information (e.g., balances and transaction history) and make payments
  - Member statements
  - Check re-ordering

  - Change address
  - Send secure messages to the Credit Union
  - Person-to-Person transfer via PayPal
  - Personal Financial Management software
  - Online bill paying services
  - Electronic retrieval of check copies
- Mobile Banking
  - View account balances
  - View transaction history
  - Transfer funds between accounts at the Credit Union
  - Transfer funds to other Credit Union member accounts (pre-authorization required)
  - Transfer funds to parties outside the Credit Union
  - Mobile Deposit
  - Account alerts
  - Find the nearest Credit Union branch, shared branching location or Co-op ATM location
  - Person-to-Person transfer via PayPal
  - Personal Financial Management software
  - Online bill paying services
  - Electronic retrieval of check copies
- Audio response/phone-based (Telephone Banking)

E-COMMERCE SAFEGUARDS

It is the practice of Resource One Credit Union to safeguard member data at all times, including during 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.

Strategically-Placed Web Servers

The Credit Union's website is entirely separate from the core processing system. There is no direct connection from the website server to the internal computer system. Scanning systems are in place to detect any attempted unauthorized access, attacks, and system intrusions.

Any publicly addressable server or system that requires access from the Internet must be isolated through the use of a web server. The web server must go back through the firewall for access to the network. The web server will talk to the application on the same network.

Firewalls

The firewall is a security measure which governs access control and protects the internal system from compromise. All information, both into and out of the Credit Union's core processing center, passes through this firewall. Firewall configuration is the responsibility of the third party vendor.

- The Credit Union shall deploy and utilize firewalls as necessary to protect internal systems from threats originating from the Internet as well as those that might be present when connecting to vendors' networks.
- Firewall operating systems and configurations will be reviewed as defined within the *Perimeter Network Security* section of this document to ensure maximum protection.
- All attempts to access un-configured (blocked) services will be documented and monitored.

- Network Traffic Rules and Restrictions
  - Intra-network traffic is subjected to distinct operating rules and restrictions.
  - Through the use of firewall technology, outside parties are directed only to approved internal resources. This strategy dramatically reduces the risk of any party gaining unauthorized access to a protected server.
  - The internal network is also protected from virus attacks through the use of network-level antivirus software that is updated automatically on a regular basis.
  - E-mail is also scanned prior to delivery, reducing the potential of a virus entering the network in this manner.

TECHNOLOGY PLAN

The Credit Union will develop and maintain a formal Technology Plan that aligns with the Credit Union's Strategic Plan and will include short term plans, long term plans, and resource assessments. The Technology Plan will be approved by the Technology Committee, reviewed on an annual basis, and updated as necessary to ensure it remains relevant. The Credit Union will include all e-commerce activities in business resumption planning.

LEGAL/COMPLIANCE REVIEW

The Credit Union will review legal and compliance requirements for each contemplated e-commerce activity. Legal counsel will be consulted when determined appropriate by Credit Union management. Procedures will be put in place to ensure that e-commerce transactions are legally binding before implementation.

WEBSITE OPERATING STANDARDS

The Credit Union maintains a consumer website as a vehicle to provide information on the Credit Union and Credit Union services to the general public and member access to services such as Internet Banking and Bill Pay. It also affords the Credit Union an effective method of providing Credit Union news and announcements. The Credit Union uses the website to provide information on security alerts, forms, and educational information as well as information on other educational opportunities, such as financial seminars.

Website Hardware and Software

All hardware and software used in providing and maintaining the website must be approved by the Director of Information Technology. The IT and Marketing Departments in coordination with the Credit Union's website vendor, Rackspace, will be responsible for the administration, installation, and maintenance of the approved hardware and software.

Website Content

All website content must be reviewed and approved by the senior management or Compliance Officer before posting. Content will generally be limited to products and services provided by the Credit Union, information about the Credit Union, news and announcements, member information, and educational materials. A copy of each approved page will be retained on file until such time the page is revised or deleted. The name and signature of the approver and the date approved should be noted on each page or retained within an email archive.

Any time the content of a page is to be revised and includes verbiage pertaining to compliance and/or regulatory disclosures, the proposed change must be reviewed and approved by senior management or Compliance Officer before the change is made to the website. A electronically-scraped copy of the revised page with the approver's name, signature, and date approved will be retained on file.

Once a page has been approved, it will be posted to the Credit Union website by the website administrator. Once the page is on the Credit Union website, the page will be reviewed to ensure that what has been posted is exactly what was approved. A copy of the page will be scraped from the website, the final review date will be noted on the electronically-scraped page, and a copy will be retained with the originally approved page.

In addition to each approved page, a list of all approved changes will be maintained by the Marketing Department.

Website Links to External Sites

All external links provided on the Credit Union website must be approved by senior management or the Compliance Officer. The destination site for each external link will be reviewed for content and appropriateness before the link is made available through the Credit Union website.

A list of all approved external links will be maintained by the Marketing Department. This list of approved external links will include the name of the linked company, organization, or individual along with the website address and date of the approval.

The Credit Union will display a notice to the viewer that they are leaving the Credit Union website prior to providing access to an external website through the use of a speed bump or an interim page.

Website Monitoring

The Marketing Department is responsible for monitoring the website for unauthorized changes, broken links, and any other issues. External links and website content will be reviewed monthly. Web-linking relationships will be monitored to ensure only those companies, organizations, and/or individuals who have been properly approved are listed on the website.

The Director of Marketing will be notified of any issues that could potentially have a significant impact to members.

Website Privacy Notice

The Credit Union will maintain a Website Privacy Notice that will be conspicuously posted on the website. The notice will contain information on whether or not the Credit Union accepts cookies, the Credit Union's policy in regard to privacy for both members and non-member visitors to the website, information on third party links, email, etc.

Website Compliance Review

A website compliance review is performed at least annually by either a third party vendor or Credit Union personnel having no responsibility for the development or maintenance of the website. The compliance review will be performed to ensure compliance with appropriate regulations, such as Truth in Lending, Truth in Savings, advertising, etc.

INTERNET BANKING ACCESS

The Credit Union will utilize an Internet Banking module that will be maintained and serviced by a third party provider (PM Systems). The Internet Banking platform utilizes an SSL Certificate issued by Comodo to protect communications between the PM Systems Internet Banking server and website visitors. This will encrypt the communication sessions and also allow for the visitor to verify that the website is really that of the Credit Union and not a fraudulent website.

The Credit Union supports 2048-bit SSL for electronic banking. Access to Internet Banking services will be restricted to those members using a web browser with an appropriate encryption capability.

Administrator Access

Varying levels of administrator access to e-commerce applications will be restricted to the authorized third party vendor as well select IT, Accounting, Marketing, and Remote Center staff members who may assist with maintenance of the system and have a signed *Special Access Agreement* on file in the personnel records. Special access guidelines and dual control and segregation of duties standards as outlined elsewhere in this document will be followed.

Employee Access

Employee access is restricted to the employee's own account(s) in the same manner as any other member has access to their own account. Credit Union Contact Center personnel have the ability and authority to reset member passwords in the event a member forgets a password.

Know Your Member Compliance

Only existing members will have access to Internet Banking.

INTERNET BANKING AUTHENTICATION

After a secure connection is established, the initiating party must prove their identity prior to conducting the transaction by entering account number along with password. In order to comply with stricter rules concerning authentication, the member must initially chose and provide answers to member-defined challenge questions. If the member attempts to gain access to the Internet Banking system on a computer other than the one used to gain initial access (the original computer used to provide the answers to the challenge questions), the system will automatically display the challenge questions. The member must further authenticate by correctly answering the challenge questions.

Internet Banking Passwords

Members participating in Internet Banking will be required to select a unique password. Use of this password is the required security procedure to access Internet Banking through any equipment.

Internet Banking passwords will be a minimum of seven (7) characters in length. For security purposes, the Credit Union will discourage members from using:

- Member's name or social security number.
- Account number.
- Telephone number.
- The same password that that is used on other Credit Union products such as the automatic teller machine.

Other Internet Banking controls include:

- Internet Banking access will be blocked for one (1) hour after three (3) failed logon attempts. After a total of five (5) consecutive unsuccessful logon attempts the account will be disabled, requiring the member to contact the Credit Union where a Remote Center representative will reset the account after correctly answering a series of identification verification questions.
- Internet Banking sessions will be terminated after ten (10) of inactivity. The timeout period may be not be modified by the member.
- The Credit Union provides Internet Banking users with educational initiatives regarding mobile device security (e.g., establishing a strong passcode on the device used for Mobile Banking).

INSTANT DEPOSIT (INTERNET BANKING)

The Credit Union provides remote deposit services to participating members through the Internet banking platform. Member access to Instant Deposit is accomplished solely from the Credit Union's Internet banking platform to which the member has already logged on with the appropriate user ID and password. Because the only access to Instant Deposit is through the Internet Banking platform, additional authentication to the Instant Deposit application is not required.

After logging on to Internet banking, to start the remote deposit process, the user selects Instant Deposit. A page appears containing a drop down screen from which the user selects the target deposit account. The Credit Union utilizes a non-scan method, in which the user is required to enter the check number, check date, and check amount. Once the deposit has been accepted, a transaction receipt page is displayed with a batch number. The member is then required to mail the check to the Credit Union. The batch number must be written on the return envelope.

Controls

The following Instant Deposit controls used by the Credit Union include:

- Drop down screen provided containing only the user's accounts for selection.
- Daily deposit limits as determined by the Credit Union.
- Travelers Cheques, cash, and U.S. Savings bonds will not be accepted.
- No remotely deposited items will be accepted at any teller window or through the ATM or night drop.
- Deposit Item(s) must be received within five (5) business days or deposit will be reversed. An email is sent to the member with the explanation of the adjustment and notations will be made on the account.
- Repeated product abuse will result in termination of this feature.

Confidentiality

The Credit Union's Internet Banking Privacy Policy will be provided to members when they receive Internet Banking access and it will also be posted on the Credit Union's website. The contracts with the providers of electronic banking software will require that member information be kept confidential.

MOBILE BANKING

Resource One offers a mobile website (WAP) as well as downloadable mobile applications where members with internet-enabled mobile devices. All Mobile Banking sessions will utilize a minimum of 128-bit SSL encryption for all communications.

Enrollment & Authentication

Members who wish to enroll in Mobile Banking must do so within Internet Banking after authentication. To login to Mobile Banking, members must use the same username and password used to authenticate to Internet Banking. Additionally, the mobile device used to access Mobile Banking must also be configured to accept cookies in order to allow the platform to successfully identify the device.

Other Controls

- After three (3) unsuccessful logon attempts, the member will be locked out of Mobile Banking and will need to call the Credit Union to have their account reset.
- The Mobile Banking session will timeout after five (5) minutes of inactivity, requiring the user re-authenticate.
- The Credit Union provides Mobile Banking users with educational initiatives regarding mobile device security (e.g., establishing a strong passcode on the device used for Mobile Banking).

Mobile Deposit (Mobile Banking)

The Credit Union provides remote deposit services to participating members through the Mobile Banking. Member access to Remote Deposit Capture is accomplished solely from the Credit Union's secure mobile banking website or application to which the member has already logged on with the appropriate user ID and password. Because the only access to Mobile Deposit is through Mobile Banking, additional authentication to the Mobile Deposit application is not required.

After logging on to Mobile banking, to start the remote deposit process, the user selects Mobile Deposit. A page appears containing a drop down screen from which the user selects the target deposit account. The user is required to enter the amount of the check and then take a picture of the front and back the check. During the scanning process, a series of procedures take place that assess risk (stale checks, duplicate numbers, etc.). After scanning, the user is provided the transaction details and must confirm or cancel the deposit. Once the deposit has been accepted, a transaction receipt page is displayed.

- Controls

  The following Mobile Deposit controls used by the Credit Union include:

- Drop down screen provided containing only the user's accounts for selection.
- Daily deposit limit as determined by the Credit Union.
- Deposits of checks dated more than six (6) months prior to scan date will not be accepted.
- Foreign checks and U.S. Savings bonds will not be accepted.

ELECTRONIC STATEMENTS

Electronic statements will be offered to participating members utilizing the services of a third party service provider. The third party service provider will be required to meet or exceed stringent security, confidentiality, and contract requirements.

Member Access to E-Statements

Electronic statements will be provided on a normal statement cycle for members who request this service. Members will be notified via email that their e-statement has been processed and is ready for retrieval.

BILL PAYMENT

Bill payment services will be offered to participating members utilizing the services of a third party service provider. The third party service provider will be required to meet or exceed stringent security, confidentiality, and contract requirements established under the *Contract Provisions and Oversight of Third Party Providers* section of this document.

Single Sign-On Access to Services with Internet Banking

Member access to select services is accomplished solely from the Credit Union's secure Internet Banking platform to which the member has already logged on with the appropriate account number and password. Because the only access to these services is through the Internet Banking, additional authentication to these sites is not required.

These services include:

- Online Bill Pay
- Personal Financial Management
- E-Statements

Risk and Controls

The Credit Union will maintain e-commerce bill payment procedures consistent with the risk and controls associated with underlying payment systems (check processing, ACH, wire transfer, etc.).

LOAN APPLICATIONS

Members and non-members may apply for loans from the Credit Union's website. Once the applicant completes the loan application request, the form is emailed to the Credit Union. Upon receipt, the Credit Union's usual loan approval process will begin.

TELEPHONE BANKING

Telephone Banking is provided through a Credit Union-maintained and serviced system and includes the following services:

- Hear account balances
- Review transaction history
- Transfer funds between the member's share and share draft accounts
- Transfer funds between two member accounts (pre-authorization required)
- Order a stop payment on a check
- Withdrawal by check

Authentication

Users must enter their account number followed a four-digit PIN. The session will be closed after three (3) invalid sign-on attempts. Following a lockout, the member must contact the Credit Union to have the account unlocked by a Remote Service representative after successfully answering a series of identification verification questions.

Other Telephone Banking Controls

Other Telephone Banking controls include:

- Telephone Banking allows three (3) bad PINs then it says, "Please contact the Credit Union for service" and hangs up.
- After ten (10) seconds of no response, the Telephone Banking menu will be repeated twice. If still no response, the session will be closed.
- Checks will be only issued to the account holder and only sent to the address on record.

PERFORMANCE

Management will monitor totals of e-commerce services (i) to verify that the programs are cost beneficial; (ii) to incorporate the results into strategic and operating plans, budgets, and other analyses; and (iii) to consider the impact of e-commerce activity on funds management, liquidity, and interest rate risk.

The Credit Union will maintain reports that capture the following information:

- Transaction volumes by type, number, dollar amount.
- Credit performance and profitability of loan accounts originated through the Internet.
- Intrusions, both attempted and actual.
- Member complaint volumes and average time to resolution.

RECONCILIATIONS

All activity with Internet Banking vendors will be balanced in accordance with the Credit Union's internal control program and account reconciliation procedures.

RISK ASSESSMENT APPROACH

Resource One will take a risk-based approach to evaluating e-commerce services and will conduct initial and ongoing risk assessments of E-Banking (Internet, Mobile Banking,) activities. Initial risk assessments will identify the strategic, transactional, compliance, and reputation risks and mitigating factors associated with potential e-commerce activities.

Risk assessments will be performed on a periodic basis, but at least annually, and will determine the risks associated with each product and service and will ensure that appropriate controls have been implemented that will mitigate the associated risks. The risk assessment should include a review of authentication tools for each e-commerce product or service offered. Where risk assessments indicate single-factor authentication is inadequate, multifactor authentication, layered security, or other controls will be implemented.

Application Vulnerability Assessment

Application vulnerability assessments (including security) will be performed periodically for web-based applications developed specifically for the Credit Union under contract. For web-based applications provided by a vendor, the Credit Union will review any application test and/or audit summaries to ensure the application provides appropriate security and that vulnerabilities are identified and corrective action taken.

Internet and Mobile Banking Vulnerability Assessment

The Internet and Mobile Banking vulnerability assessment will be conducted on at least an annual basis. The vulnerability assessment will consist of an inspection and analysis of the security controls in place to prevent unauthorized transactions and unauthorized access to non-public member information.

Remote Deposit Capture (Instant & Mobile Deposit) Risk Assessment

Credit Union management will incorporate their risk assessments of the remote deposit capture service into existing risk assessment processes.

The remote deposit capture risk assessment will be reviewed on an annual basis and updated as technology, market, member base, industry, or processes change. The risk assessment will encompass factors such as the anticipated volume of remote deposit capture transactions and will involve all relevant functional areas of the Credit Union to ensure all the risks have been identified and reviewed including legal, compliance, reputation, and operational risks.

Problem Resolution and Escalation Process

Primary responsibility for problem resolution will be assigned under each e-commerce service identified. If a problem cannot be solved at that level, the following steps will be taken:

- Notification of all applicable department heads
- Escalate problem resolution to senior management team.

Contract Provisions and Oversight

The Credit Union will exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented effective, secure, reliable e-commerce solutions. New contracts will contain a brief description of work to be performed; require the service provider to implement and maintain adequate security measures; contain assurances of performance, reliability, disaster recovery capabilities; and reporting requirements which could include performance, security evaluation summaries, and must include reporting any breach of sensitive member information as defined by 12 CFR Part 748 Appendix B - Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice.

STAFF TRAINING AND REVIEW

IT and other appropriate staff shall receive periodic training and review all procedures as major system additions or changes are implemented.

REPORTING

E-commerce issues will be included in periodic reports to the Technology Committee including technologies employed, risks assumed, and compensating risk management controls that have been implemented.

Management reports will include the measure or analysis of e-banking performance both strategically and technically, such as the percentage of members using e-banking channels or system capacity to maintain current and planned level of transactional activity.

The Technology Committee will periodically review e-banking-related security reports including suspicious activity, unauthorized access attempts, outstanding vulnerabilities, and fraud or security event reports, etc., including documentation related to any successful e-banking intrusion or fraud attempt.

Historical Record of Policy Changes

Date Rewritten: July 2013
Date Ratified: July 2013

This policy is a complete rewrite.

INDEX