4300. UNAUTHORIZED ACCESS TO MEMBER INFORMATION POLICY

TABLE OF CONTENTS

Purpose/Authority

This policy, in compliance with NCUA Part 748, Appendix B, addresses the increasing number of breaches or attempted breaches of member information that has resulted in the rapid escalation of identity theft over the past several years. Pursuant to this guidance, the Board of Directors and Management of Resource One Credit Union has implemented this policy in a spirit of compliance and security.

Statement

Resource One Credit Union Management, facilitating the protection of member funds and information, has reviewed, developed and implemented strategies to address industry concerns resulting the increasing level of unauthorized access to member information and resulting identity theft.

Definitions

- Management - President, Chief Financial Officer, other officers or managers with appropriate decisional authority to specifically handle these situations.
- Member information systems - Includes all the methods used to access, collect, use, transmit, protect, or dispose of member information, including the systems maintained by service providers.

Applicability

Using guidance from Appendix B to Part 748, "Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice", we adhere to the following policy to maintain and protect member information from unauthorized access:

Response Program

In situations where information security has been breached, management will:

1. Assess the situation identifying member information systems and types of member information that appears breached. Notify the NCUA Regional Director as soon as possible when made aware of an incident involving a breach of "sensitive" member information to include:
   - name
   - address
   - telephone number
   - social security number
   - driver's license number
   - account number
   - credit/debit card number
   - personal identification number or password accessing the member's account any combination of information that would permit logging onto or accessing the member's account (ex., user name with password or password with account number.)
2. File a Suspicious Activity Report (SAR) and notify appropriate law enforcement authorities.
3. Take measures to prevent further unauthorized access to/use of member information by monitoring (if feasible), freezing, or closing affected accounts, while preserving records and other evidence.

4. Provide notice as soon as possible to members after determination of unauthorized access to sensitive member information and the likelihood of its misuse.

   - Notice may be delayed if advised in writing by the appropriate law enforcement agency that notification will interfere with a criminal investigation. Notification of the member will occur upon confirmation from law enforcement that notification will no longer interfere with the investigation.

   - Notification may be limited to only those individuals whose information has been breached if investigation reveals, from logs and other data, specific members' information that has been improperly accessed.

   - Management will determine the most efficient method of notification according to the existing circumstances, which includes telephone, mail, or electronic mail for members who agree to receive communications electronically and for whom the credit union has a valid e-mail address.

   - Notice to be provided affected members is attached (See PROCEDURES – UNAUTHORIZED ACCESS TO MEMBER INFORMATION)

INDEX