WEBSITE PRIVACY NOTICE

By using our web site or interacting with an advertisement or page, you consent to this Policy, including your consent to our use and disclosure of information about you in the manner described in this Policy.

Fraternal Order of Police Credit Union respects the personal and financial privacy of all of its members. We are committed to protecting the information on and within our web site with the same safety and confidentiality standards utilized in the transaction of all Fraternal Order of Police Credit Union business. The following information will help you to understand how we protect the information gathered.

Fraternal Order of Police Credit Union may collect information such as:

- user name
- e-mail addresses
- Internet Service Provider address
- access time and date
- failed login attempts

We collect this information for internal reporting of web site statistics, and product monitoring to improve our services. Information obtained from our web site is kept secure, and access to that information is limited with the credit union personnel who need to know the information to provide products or services to our members and to properly operate the credit union.

INTERRUPTION OF SERVICE

At certain times, Fraternal Order of Police Credit Union may not be available due to system maintenance or circumstances beyond our control.

INTERNET ACCESS FEES AND TELEPHONE CHARGES

You agree to be solely responsible for any telephone charges, internet access fees, and other such similar fees and expenses you incur by accessing Fraternal Order of Police Credit Union through this site. Please note that these fees may be assessed and billed separately by your online service provider or phone company.

CHILDREN

Fraternal Order of Police Credit Union does not knowingly solicit data from children. We recognize

that protecting children's identities and privacy on-line is important and the responsibility to do so rests with both the online industry and parents.

COOKIES

Fraternal Order of Police Credit Union does not utilize internet "cookies." Cookies are a feature of web browser software that allows web servers to recognize the computer used to access a website. They are small bits of data that are stored by a user's web browser on the user's hard drive. Cookies can remember what information a user accesses on one web page to simplify subsequent interactions with that website by the same user or to use the information to streamline the user's transactions on related web pages. Some of our associated companies may themselves use cookies on their own websites. We have no access to, or control of these cookies, should this occur.

ONLINE BANKING

If you visit our secure Online Banking site, you will be required to provide multifactor authentication (answer one of several secure questions) in addition to a Personal Identification Number (PIN) that is your unique password to enter and use our secure Online Banking server. This information is never given, sold or disclosed to third parties. It is held in strict confidence. When using Online Banking, certain online information, including the transactions you conduct, are recorded. This allows the Fraternal Order of Police Credit Union staff to confirm your transactions. The Credit Union stores no member or account information on our web server, which is accessed by the public. All member account information is housed on computers that are behind firewalls (protected area). All on-line transactions are authenticated and encrypted with the highest level of security protection available.

Your Fraternal Order of Police Credit Union information is password-protected. Fraternal Order of Police Credit Union uses industry-standard SSL encryption to protect data transmissions. Emails that you may send without logging in to Fraternal Order of Police Credit Union may not be secure. For that reason, we ask that you do not send confidential information such as Social Security or account numbers to us through an unsecured email.

We provide a number of additional security features at Fraternal Order of Police Credit Union. After logging in, your online "session" will "timeout" after 30 minutes of inactivity and you will be automatically logged off. This prevents other individuals from accessing your personal information in case you have left your PC unattended without logging out. When you submit your password, it is compared with the password we have stored in our secure database. We allow you to enter your password incorrectly three times. If you enter your password incorrectly more than three times, your

access to Fraternal Order of Police Credit Union will be locked until you contact us to reactivate the account. We monitor and record "bad login" attempts to detect any suspicious activity, such as someone trying to guess your password.

LINKS

We are not responsible for practices employed by websites linked to or from our site, nor the information, content, accuracy, or opinions expressed in such websites, and such websites are not investigated, monitored or checked for accuracy or completeness by us, nor do we maintain any editorial or other control over such websites. Inclusion of any linked website on our site does not imply approval or endorsement of the linked website by us. This remains true even where the linked site appears within the parameters or window/frame of our site. Often, links to other websites are provided solely as pointers to information on topics that may be useful to users of our site. Please remember that when you use a link to go from our site to another website, our Privacy Policy is no longer in effect. Your browsing and interaction on any other website, including websites which have a link to our site, is subject to that website's own rules and policies. We are not responsible for the data collection and practices of third parties linked to our website. Please read the rules and policies of the third-party sites before proceeding. If you decide to leave our site and access these third-party sites, you do so solely at your own risk.

EMPLOYEE SECURITY STANDARDS

Fraternal Order of Police Credit Union maintains information standards and procedures that include physical and electronic safeguards, restricting access to those trained employees on the importance of information security.

POLICY UPDATES AND EFFECTIVE DATE

If we make updates to this policy, we will update the policy with the changes and revise the “date of most recent update” posted at the top of this policy. Any updates to the policy become effective when we post the updates on the site. Your use of the site following the update to the policy means that you accept the updated policy.

GUIDELINES:

POLICY AND PROGRAM RESPONSIBILITY

A) Credit Union has established a website team, made up of the Credit Union's PRES/CEO and the board member with a marketing portfolio. This Web site Committee will maintain and monitor the Credit Union's Web site.

B) Any new Web site ideas or initiatives must be reviewed by the Web site Committee, will present any new applications to the board of directors for approval.

C) Management will establish and provide the Board of Directors with regular reports on its Web site activity and transactions.

RISK ASSESSMENT

A) The Credit Union will regularly test the efficacy or its E-commerce systems to ensure proper working order and to prevent security weaknesses.

B) The Management Team will classify the level of data sensitivity of services, technological and operational changes in E-commerce and maintain a current list of critical risk levels of security, virus detection and protection.

COMPLIANCE AND LEGAL

The Credit Union ensures that its Web site will comply with all applicable laws and regulations. The Credit Union also monitors all changes in laws and regulations that affect E-commerce, and updates its E-commerce policies, practices, and systems accordingly in a prompt manner.

A) The Credit Union has secured bond coverage for all of its Web site policies and procedures. Management has ensured that bond coverage is sufficient in the event of any loss due to an electronic transaction. Bond coverage is regularly assessed to ensure the sufficiency of coverage.

B) The Credit Union will provide various Web site contracts and agreements to in-house auditors and federal examiners.

C) The Credit Union maintains a Web site privacy disclosure that is available to all members who visit the Credit Union Web site.

D) The Credit Union monitors and enforces compliance with its Web site privacy disclosures. In addition, the Credit Union Web will place appropriate warnings on its Web site, clearly stating that unauthorized access or use of the Web site is not permitted and may constitute a crime punishable by law.

AUDIT AND CONSULTING SERVICES

A) The Credit Union's Web site activities will be subject to annual independent audits. At a minimum, these reviews will cover Web site: security, penetration testing, regulatory compliance, and maintenance.

B) The Credit Union management will correct the issues of concern uncovered by the independent audit and/or quality review.

C) The Credit Union will regularly require performance testing of its Web site to identify and prevent potential vulnerabilities.

VENDOR MANAGEMENT

A) The Credit Union has obtained a vendor to install and/or maintain its Web site. The Credit Union has exercised due diligence in selecting its vendor to ensure that proper security measures are in place to protect member account information.

B) The Credit Union will develop procedures to monitor vendor relationships to ensure that they continue to meet the needs of the Credit Union (i.e., hardware, software, network services, content accuracy, availability, usability, security, and privacy.)

MEMBER SERVICE AND SUPPORT

A) Management will take steps to ensure that staff is adequately trained in order to address member support issues.

PERSONNEL

A) Employees with access to member account information will receive a copy of the Credit Union's Web site policy, must sign a compliance policy statement (confidentiality and information security) when hired by the Credit Union. Employees will be notified of the importance of maintaining the confidentiality of member account information and will be made aware of the Credit Union's policies, procedures, standard practices, and disciplinary actions that will be taken against the employee for non-compliance with the Credit Union's privacy and information security policies and procedures. The Credit Union policy prohibits staff from inappropriately disclosing member account information to any third party.

B) The Credit Union limits access to sensitive information to specific employees to ensure confidentiality of member account information. Employees have been trained on the proper procedure for filing reports to the appropriate regulatory and law enforcement agencies. Management will routinely monitor employees for compliance with Credit Union's state policies, procedures, and standards.

C) The Credit Union has conducted background checks on its employees, and will thoroughly investigate any allegations of employee misconduct.

D) Management has implemented procedures and training with employee support, in the event of termination, transfer, promotion, etc. Employees involved with the Credit Union's Web site transactions are kept up-to-date with changes in the policies and procedures of the Credit Union.

SYSTEM ARCHITECURE AND CONTROLS

A) The Credit Union maintains an inventory of hardware and software to ensure continuity of service in the event of a technological failure, natural disaster, or intentional destruction of its electronic systems. The Credit Union (or its vendor) maintains procedures to allow the Credit Union to restore its previous configuration in the event a software modification adversely affects the Web site.

B) The Credit Union has implemented a disaster recovery system as part of its business continuity plan. This system will be monitored regularly and updated as needed as a result of changes in technology, legislation, and infrastructure.

FRATERNAL ORDER OF POLICE CREDIT UNION

SECURITY INFRASTRUCTURE AND CONTROLS

A) The Credit Union maintains security measures consistent with the requirements of federal and state regulations, including risk management systems designed to prevent unauthorized access, both internal and external, to member information.

B) The Credit Union has procedures in place to protect the member's information, in the event of natural disasters, intentional destruction, or technical failure.

C) Management monitors employees with access to members' account information to ensure they are in compliance with the Credit Union procedures.

D) All member account information is stored on servers protected with Enter Protection Software or Hardware to prevent unauthorized access and/or damage. The protections are monitored on a regular basis to assess potential security weaknesses.

E) Access to member accounts is restricted to members through the use of user ID numbers and passwords. Account passwords that are not entered correctly after the Enter Time Period, generally in minutes time will result in an automatic log off to the session.

F) The Credit Union has implemented an intrusion detection system to monitor activity and alert the credit union immediately in the event of a security breach. The Credit Union's oversight committee has been trained to handle such breaches in a timely and effective manner.

PERFORMANCE MONITORING. The Credit Union has established and implemented performance standards and monitoring procedures for its Web site activities. These standards and procedures are designed to ensure that the Credit Union's E-commerce and Web site activities are available and efficiently meet member needs and expectations. The procedures are updated on a regular basis, as a result of changes in long term and short term plans, as well as in response to member needs.

USA PATRIOT ACT

Customer Identification Requirements

In accordance with section 326 of the USA Patriot Act, enacted October 2001, to protect you, your family and our country from terrorism by preventing terrorism financing, all applicants for new accounts are required to provide current picture identification that verifies identity including name, address, and other identifying information. We must also verify the identity of persons added as joint owners to and who have access to new or existing deposit accounts or loans. We must also retain records of the documents used to verify your identity.

In some cases, identification will be requested for current account holders if original documentation was not obtained with the opening of the account or the account was opened prior to enactment of the Patriot Act.

In all cases, protection of our member accounts and confidentiality is our concern as we work to maintain the security of your funds and our country.

Please speak with a credit union employee if you have any questions or concerns about our requirements of this policy.