**SECURITY STATEMENT/VIRTUAL BRANCH HOME BANKING & E-MAIL**

The Empire ONE Federal Credit Union is pleased to offer home banking services via the Internet. Delivering these services requires a solid security framework that can protect you and our institution from outside intrusion. The information below summarizes our security framework, which incorporates the latest proven technology. A section at the end also summarizes your responsibilities as a user of the home banking system with regard to security. There are several levels of security within our security framework. User Level deals with cryptography and Netscapeís Secure Sockets Layer (SSL) protocol, and is the first line of defense used by all members accessing our Home Banking Server from the public Internet. Server Level focuses on firewalls, filtering routers, and our trusted operating system. Host Level deals specifically with our home banking services, and the processing of secure financial transactions.

**USER LEVEL**

There are several components of User Level security that ensure the confidentiality of information sent across the public Internet. The first requires your use of a fully SSL-compliant browser such as Netscape Navigator or Microsoft Internet Explorer. SSL is an open protocol developed by Netscape that allows a userís browser to establish a secure channel for communicating with our Internet Server. SSL utilizes highly effective cryptography techniques between your browser and our server to ensure that the information being passed is authentic, cannot be deciphered, and has not been altered en route. SSL also utilizes a digitally signed certificate which ensures that you are truly communicating with the Home Banking Server and not a third party trying to intercept the transaction.

After a secure connection has been established between your browser and our server, you then provide a valid User ID and Security Code to gain access to the services. This information is encrypted, and a request to log on to the system is processed. Although SSL utilizes proven cryptography techniques, it is important to protect your User ID and Security Code from others. We recommend using a full 8-digit security code and changing it often. Session time-outs, a limit on the number of logon attempts, forced Security Code change intervals, and special browser caching techniques are examples of other security measures in place to ensure that inappropriate activity is prohibited at the User Level.

**SERVER LEVEL**

All transactions sent to our Home Banking Server must first pass through a filtering router system. These filtering routers automatically direct the request to the appropriate server after ensuring the access type is through a secured browser and nothing else. The routers verify the source and destination of each network packet, and manage the authorization process of letting packets through. The filtering routers also prohibit all other types of Internet access methods at this point. This process blocks all non-secured activity and defends against inappropriate access to the server.

The Home Banking Server is protected using the latest and most powerful firewall platform. This platform is based on a government-rated B1 trusted operating system, in use for many years by high-security government agencies including the U.S. Department of Defense. This platform defends against every kind of system intrusion and effectively isolates all but approved member financial requests. The platform secures the hardware running the home banking applications and prevents associated attacks against all systems connected to the Home Banking Server. Administration of the platform cannot occur remotely and must be initiated by authorized personnel in direct physical contact with the master

console. Thus, a level of physical security has been implemented that rivals some of the most secure government facilities. Additional measures to ensure the security of information involve the separation of server applications from host data. This means that information of value does not physically reside on the Home Banking Server. Logging of security information occurs at all times and there is always a backup of the information logged including every attempt made to access the system. These security logs allow us to constantly monitor for a wide range of anomalies and to determine if attempts have been made to breach our security framework.

**HOST LEVEL**

After passing through the Home Banking Server, the transaction is sent via secure dedicated communication lines to our Transaction Server that verifies member identity. Once authenticated, the member is allowed to process authorized home banking transactions using host data. No direct database access occurs between the Home Banking Server and the Transaction Server. Only specific transactions in the proprietary format are allowed into the Transaction Server. Protocol conversions have also been implemented to ensure that information does not remain in a single state of existence, further securing the information at any given point in the transaction process. In addition, communication time-outs ensure that the request is received, processed and delivered within a given timeframe. Any outside attempt to delay or alter the process will fail. Further password encryption techniques are implemented at the Host Level, as well as additional security logging and another complete physical security layer to protect the host information itself.

**USER RESPONSIBILITIES**

While we continue to evaluate and implement the latest improvements in Internet security technology, users of the Home Banking System also have a responsibility for the security of their information and should always follow the recommendations listed below:

• Utilize the latest version of either Netscape Navigator or Microsoft Internet Explorer. The Home Banking System is best viewed and is most secure when you use one of these two browsers, as they are both certified for use at our site.

• Your Security Code must be kept confidential. Utilize a full 8-digit Security Code and change it frequently to ensure that the information cannot be guessed or used by others.

• Be sure others are not watching you enter information on the keyboard when using the system.

• Never leave your computer unattended while logged on to the Home Banking System. Others may approach your computer and gain access to your account information if you walk away.

• Click Exit when you are finished using the system to properly end your session. Once a session has been ended, no further transactions can be processed until you log on to the system again. • Close your browser when you are finished, so that others cannot view any account information displayed on your computer.

• Keep your computer free of viruses. Use virus protection software to routinely check for a virus on your computer. Never allow a virus to remain on your computer while accessing the Home Banking System.

When you follow these simple security measures, your interaction with the Home Banking System will be completely confidential. We look forward to serving your home banking needs for both today and into the future and securely!

**VIRTUAL BRANCH E-MAIL vs. WEB SITE E-MAIL**

Empire ONE Federal Credit Union web site provides addresses that allows you to communicate with us through the convenience of e-mail. Unfortunately, there is currently no widely accepted method of encrypting e-mail originating directly from our web site. Because of this, we advise you not to include any confidential information in your web site e-mail correspondence. This includes Social Security numbers, account numbers, PIN numbers or Security Codes, etc. If you wish to communicate sensitive or personal information via the Internet, you are welcome to use our secure e-mail service available through Virtual Branch Home Banking, which is called E-Mail. E-Mail is an encrypted communication tool for confidential information. You must have access to Virtual Branch Home Banking in order to utilize E-Mail by completing and submitting a signed Virtual Branch Home Banking Application.