

# PRIVACY POLICY

## **1<sup>ST</sup> Valley Credit Union's Web Site Privacy Policy**

1<sup>st</sup> Valley Credit Union is committed to protecting the privacy of its members and other users of its web site. To that end, the Credit Union has adopted the following privacy policy for its web site:

Online Privacy: We do not gather user specific information details from your computer Internet software or save data about you and your computer when you visit our public web site at **www.1stValleyCu.com**, other than what is needed to authenticate consumer access to our Virtual Branch home banking products. Our site uses browser cookies only after you have logged into Virtual Branch to keep track of your transaction status or menu positions. We do not store cookies on your computer after you have logged out of Virtual Branch. On Line Security: Our site has security measures in place to protect against loss, misuse and alteration from accessing your data, and to ensure that you receive the data intact. Our web site contains practices or content of other such sites.

In Compliance with the Children's O-Line Privacy Act (COPPA), 1<sup>st</sup> Valley Credit Union does not collect personal information from children.

## **Security and Protecting Your Account**

1st Valley Credit Union is strongly committed to protecting the security and confidentiality of our member account information. We use state of the art technology in the ongoing development of its 1st Valley Credit Union Bill Payment Service to ensure security and privacy. In order to access Bill Payment Service you must have a browser that supports 128-BIT encryption.

## **User ID and Security Code**

Upon enrollment, you will be issued a User ID and eight (8) digit Security Code.

## **About Security**

We are pleased to offer Bill Payment 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 Internet Banking System with regard to security.

There are several levels of security within or security framework. User Level deals with cryptography and Netscape's Secure Sockets Layer (SSL) protocol, and is the first line of defense used by all members accessing our Internet Banking Server from the public Internet. Server Level focuses on firewalls, filtering routers, and our trusted operating system, host level deals specifically with our Internet 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 user's 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 that ensures that you are truly communicating with the Internet 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 of 3 attempts 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 Internet Banking Server must first pass through a 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 Internet 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 Internet Banking applications and prevents associated attacks against all systems connected to the Internet Banking Server.

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 Internet Banking Server. Logging of security information occurs at all times and there is always a backup of the information logged about 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 Internet Banking Server, the transaction is sent via secure dedicated communication lines to our Transaction Server, which verifies member identity. Once authenticated, the member is allowed to process authorized Internet Banking and bill payment transactions using host data. No direct database access occurs between the Internet 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 time frame. 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.

### **Your Responsibility**

- Not to give out your identifying information such as your PC password to any other person.
- Never to leave your account information displayed in an area accessible by others.
- Never leave your PC unattended while using the Bill Payment Service.
- To always exit and sign off the system properly.
- To notify the 1st Valley Credit Union at 909-889-0838 immediately if you suspect that your password has become known to any unauthorized person.

- That you understand that by using the Bill Payment Service you have agreed to the terms and conditions of this agreement.
- To use the Bill Payment Service solely as provided in this agreement.
- That 1st Valley Credit Union may download certain information to your computer or other access device, including customer identification information.
- To properly maintain any accounts you have with 1st Valley Credit Union, to comply with the most recent membership account agreement information brochure governing these accounts.
- To pay any fees incurred by the use or maintenance of your accounts.

### **Member Liability**

If you fail to maintain security of your User ID and Security Code and the Credit Union suffers a loss, we reserve the right to terminate service to you under this agreement, as well as to terminate other deposit and loan services. 1st Valley Credit Union will not be responsible for any losses you suffer due to your failure to maintain the security of your User ID and Security Code. Users of the service should use such other security code protection precautions as may be appropriate under any particular set of circumstances to ensure proper security over system access and access to account and transaction information.

This service provides the capability for you to change your security code. To help safeguard your security, you should change your security code. If you forget your security code or your system access is disabled due to the use of an incorrect security code, you must contact the 1st Valley Credit Union to request that a temporary security code be issued to you. We reserve the right to require written re-application for a new and/or replacement security code.

### **External Links Disclaimer**

When you leave 1<sup>st</sup> Valley Credit Union's Web site:

You should know that links from our Web site to external Web sites are not under the control of 1<sup>st</sup> Valley Credit Union. We can make no representation concerning the content, quality, safety or suitability of these sites or their contents, nor are we liable for the content or availability of external Web sites. These links are listed only as a convenience to our members.