



# FedLine® Web Security Overview for Users

*In today's world of rapidly developing technology, you need online access to Federal Reserve Financial Services that is designed to be both innovative and secure. With FedLine Web, you can rest assured that security is a top priority at the Federal Reserve. Making data security a top priority at your institution will help maximize FedLine Web's security features and help you get the most out of those features.*

## FedLine Web security features include:

- Credentials (digital certificates with passwords and user IDs and passwords)
- Firewalls
- Intrusion detection
- Secure Socket Layer (SSL) encryption
- Security reviews

## Credentials

The Federal Reserve uses credentials to permit only those authorized by their institution, Subscribers, to access Federal Reserve Financial Services via FedLine Web. Different types of credentials are required for access to different services. The three types of credentials that the Federal Reserve issues are: 1) digital certificates, 2) user IDs and passwords, and 3) a combination of both digital certificates and user IDs and passwords.

### Digital Certificates with Passwords

A digital certificate is equivalent to an ID badge that allows those authorized by their institution

to conduct business on the Web. When a staff member at your institution is authorized to access certain FedLine Web services as a Subscriber, the Federal Reserve provides that individual with a “badge” or certificate. This certificate should be loaded on a secure computer that the Subscriber will use to access FedLine Web. When the Subscriber logs on to FedLine Web, Federal Reserve servers check the Subscriber's computer for the certificate before granting access. Use of the certificate is protected by a password. Subscribers must enter their individual password each time they log on to FedLine Web. Strict parameters for password construction help to prevent unauthorized access.

### User IDs and Passwords

User IDs and passwords, rather than digital certificates, are required for some informational FedLine Web services. Subscribers must log on to and enter their individual password each time they access FedLine Web. User IDs allow those authorized by their institution to access FedLine Web. The use of passwords, in combination with user IDs, is intended to limit access to FedLine Web to only authorized users. Strict parameters for password construction add additional protection against unauthorized access.



## Your Role and Responsibilities

You play a critical role in protecting your computer systems and your business information. As part of your FedLine Web setup, you should use all new and existing security procedures designed to address the unique vulnerabilities of the Internet. To help protect your FedLine Web connection and the data available via the connection, at a minimum, you should:

- Prevent unauthorized access to computer systems on your premises. When preparing your computer and browser settings during FedLine Web setup, you should set a password. DO NOT use the “remember password” feature, even if it is available.
- Protect your password. Choose a password you can remember and do not write it anywhere.
- Do NOT share certificates or sessions among staff members. This practice undermines all other security efforts and eliminates your ability to know who has accessed your information.
- Install virus protection software and scan all downloaded software, as well as all diskettes, before use. You should also ensure virus definition files are up to date and delete all e-mails with attachments from unknown sources.
- Always check the Web site URL (address) to ensure it matches the FedLine Web URL before providing any confidential or security information.

For additional information concerning your responsibilities when accessing FedLine Web or using Federal Reserve Bank services, please consult the applicable Operating Circular(s), available at [www.frbservices.org/OperatingCirculars/index.html](http://www.frbservices.org/OperatingCirculars/index.html).

## Firewalls

FedLine Web uses firewalls to help protect Federal Reserve Banks’ computer systems and your information. Firewalls can be thought of as security barriers that are designed to permit only specific types of data to enter or leave Federal Reserve Bank systems. These firewalls allow for full functionality on FedLine Web, while helping to provide you with a secure environment.

## Intrusion Detection

The Federal Reserve Banks have deployed an Intrusion Detection System to constantly monitor the network for possible intrusions and unauthorized access attempts.

## Secure Socket Layer (SSL) Encryption

FedLine Web uses Secure Socket Layer (SSL) technology to help protect information during transmission. SSL is the leading security protocol for data transfer over the Internet. This technology encrypts information as it moves between your browser and our FedLine Web computer systems. To verify that your FedLine Web session is being encrypted, look for “https:” instead of “http:” in the URL address.

## Security Reviews

The Federal Reserve Banks periodically conduct security reviews of our infrastructure, as well as all FedLine Web services.

The Financial Services logo and “FedLine” are either registered or unregistered trademarks or service marks of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at [www.frbservices.org](http://www.frbservices.org).