

FEDERAL
RESERVE



FINANCIAL
SERVICES

Guide to Connectivity Options



For FedForward[®], FedReturn[®], and
FedReceipt[®] Services

Federal Reserve Banks

Version 2.4, May 7, 2008

Legal Notices

FedForward[®], FedReturn[®] and FedReceipt[®] Terms and Conditions

The terms and conditions applicable to the Federal Reserve Banks' Check Services are contained in the Federal Reserve Banks' Operating Circular 3. The terms and conditions applicable to electronic access to Check Services are contained in the Federal Reserve Banks' Operating Circular 5. Both circulars may be accessed via the Federal Reserve Financial Services Web site at www.frb services.org.

THE INFORMATION ABOUT THIRD-PARTY PRODUCTS PROVIDED IN THIS GUIDE IS PROVIDED AS-IS. THE FEDERAL RESERVE BANKS PROVIDE THIS INFORMATION ONLY AS A CONVENIENCE TO USERS AND DISCLAIM ALL REPRESENTATIONS AND WARRANTIES FOR THIS INFORMATION, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES CONCERNING SUCH INFORMATION'S ACCURACY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY AND/OR USAGE. THE FEDERAL RESERVE BANKS SHALL NOT BE LIABLE FOR ANY LOSSES, DAMAGES OR EXPENSES ARISING OUT OF USE OF, INABILITY TO USE OR RELIANCE ON SUCH INFORMATION.

Federal Reserve Banks' Trademarks

The Financial Services logo, "FedForward," "FedReturn," "FedReceipt," "FedLine," and "FedLine Web" are registered service marks of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at www.frb services.org.

Other Trademarks

"SecureTransport" is a trademark of Tumbleweed Communications Corp.

"Connect:Direct" is a registered trademark of Sterling Commerce, Inc.

"Windows" and "Internet Explorer" are registered trademarks of Microsoft Corporation in the United States and/or other countries.

"Linux" is a registered trademark of Linus Torvalds in the U.S. and other countries.

"Solaris" is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

"UNIX" is a registered trademark of The Open Group.

Table of Contents

Overview	4
Connectivity Options for Transferring ICL Files.....	5
ICL Transfer Option 1:	5
Customer-Initiated Manual Upload and Download via the Internet Using FedLine Web	5
Security.....	5
Considerations in Selecting Option 1	6
Implementation Considerations When Selecting Option 1	7
ICL Transfer Option 2:	8
Customer-Initiated Automated Upload and Download via the Internet Using Tumbleweed SecureTransport Software	8
Security.....	8
Considerations in Selecting Option 2	9
Implementation Considerations When Selecting Option 2	12
Scripting Considerations with Tumbleweed’s SecureTransport Client.....	12
ICL Transfer Option 3:	14
Upload and Download via Direct Network Connection Using Sterling Commerce Connect:Direct Secure+ Software	14
Security.....	14
Considerations in Selecting Option 3	15
Implementation Considerations When Selecting Option 3	16
Table 1: Example of Direct Network Connection Component List	17
WAN Router Information	17
Summary of Connectivity Options for ICL Transfer	18

Overview

The Federal Reserve Banks' Guide to Connectivity Options for FedForward[®], FedReturn[®] and FedReceipt[®] Services provides an overview of connectivity options for your organization and vendor personnel responsible for deploying and supporting connectivity to facilitate the exchange of image cash letters (ICL) with the Federal Reserve Banks (FRB). This document provides an overview of each connectivity option in order to assist your organization in selecting the best alternative. The document includes:

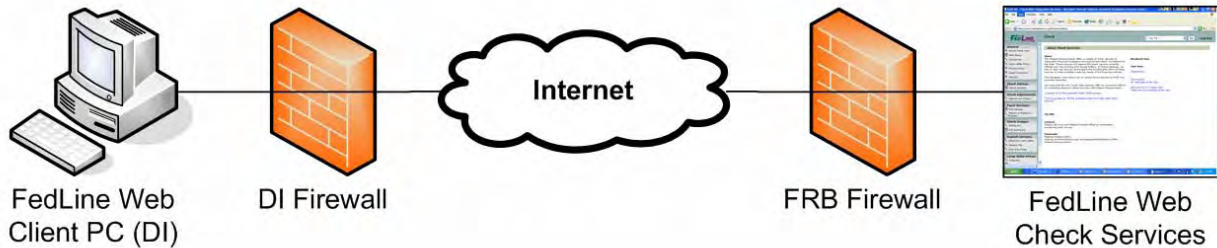
- Description of each connectivity option for ICL transfer;
- Architectural description and diagram of each option;
- Considerations for selecting the appropriate option; and
- Implementation considerations associated with each option.

The FedForward, FedReturn and FedReceipt services are Check 21-enabled clearing services that provide your organization with the opportunity to deposit and receive image cash letters. In order to facilitate efficient and effective transfer of image cash letters, the Reserve Banks have identified a set of connectivity options designed to meet the spectrum of your organization's needs. Before your organization can deliver or receive image cash letters from the Federal Reserve Banks, you must identify and implement the appropriate connectivity option and complete the enrollment and testing process for the selected FedForward, FedReturn and/or FedReceipt services. For more information on the Federal Reserve Banks' Check 21-enabled services, please visit <http://www.frb services.org/Retail/Check21.html> or contact your Account Executive. In addition, a high-level outline of the testing and implementation process is available in the Customer Implementation Guide at <http://www.frb services.org/Retail/pdf/C21ImplementationGuide.pdf>.

The options for transferring image cash letter files include the following:

- Option 1: Customer-Initiated Manual Upload and Download via the Internet using the FedLine Web[®] Access Solution. This option is primarily for organizations with daily volume of less than 2,000 checks or those able to complete file transfer within 20 minutes.
- Option 2: Customer-Initiated Automated Upload and Download via the Internet Using Tumbleweed SecureTransport[®] Software. This option is primarily for organizations with daily volume of less than 100,000 checks and those that can transfer files effectively within specified guidelines.
- Option 3: Upload and Download via Direct Network Connection Using Sterling Commerce Connect:Direct[®] Secure+ Software. This option is primarily for organizations with daily volume greater than 100,000 checks and those that can not transfer files within specified Internet guidelines on a consistent basis.

<p>Connectivity Options for Transferring ICL Files</p>	<p>Image cash letters transferred between your organization and the Federal Reserve Banks must adhere to the Federal Reserve Banks' adoption of DSTU X9.37-2003 format. For more detailed information on the format, please visit www.frbervices.org/Retail/check21TechInfo.html.</p> <p>The following sections outline the connectivity options your organization can take advantage of in order to facilitate ICL transfer.</p>
<p>ICL Transfer Option 1: Customer-Initiated Manual Upload and Download via the Internet Using FedLine Web</p>	<p>Your organization can upload or download ICLs through the Internet by logging into the FedLine Web Check Services application using a web browser. During the implementation process, users will be issued FRB security credentials¹ for the selected services to authenticate to the Check 21 environment. The following Check 21-enabled clearing services are available:</p> <ul style="list-style-type: none"> ▪ FedForward/FedReturn, which provides the ability to upload (deliver) ICLs to FRB ▪ FedReceipt/FedReturn, which provides the ability to download (receive) ICLs from FRB <p>Users accessing the FedForward/FedReturn option will be presented with a screen that allows them to upload files from their host systems. The FedReceipt/FedReturn screen contains a list of files that are available for download. The user can select a file from the list and download it to their organization's host system.</p>
<p>Security</p>	<p>Files are transferred between Federal Reserve Banks and your organization via HTTPS. Data encryption is provided by a mutually authenticated session using FRB issued credentials.</p> <p>The diagram below depicts Option 1 for your organization:</p>



¹ More information on FRB security credentials can be found on www.frbervices.org

**Considerations in
Selecting Option 1**

File transfer via the Internet using FedLine Web is only recommended for organizations with less than 2,000 checks per day or those able to complete file transfer within 20 minutes. Organizations with greater volume, those that can not complete file transfer in less than 20 minutes or those desiring faster transfer speed are strongly advised to consider implementing Option 2 in order to establish an effective file transfer process and maximize the ability to meet the desired deadlines.

File transfer via Internet using FedLine Web is a manual process requiring an operator to perform associated functions. In addition, it does NOT provide mid-file recovery which provides automatic resumption of the file transfer in the event of a communication line disruption. With this option, file transfer must be manually restarted from the beginning if there are any communication problems.

Your organization must have a connection to the Internet that can support the transfer of your daily check volume at the desired deadlines. Check image files are much larger than most other application data files. A single check, front and back, captured as a black-and-white image, is typically around 25,000 bytes, although it can vary based on the specific check stock. By identifying the number of checks in the financial institution's files and the desired transfer times, peak transfer rate requirements can be determined.

Your organization must carefully evaluate its Internet connection speed and daily usage patterns. Achievable transfer rates are impacted by many factors, but two that can have a significant influence include available bandwidth and your organization's operating environment.

Determining available bandwidth should include the following key parameters:

- Upload and download bandwidths provided by the internet service provider (ISP) may differ significantly
- Connectivity that is shared by other applications, may have different available bandwidth during anticipated transfer times
- Your organization's internal network infrastructure capacity

Determining the impact of your organization's operating environment on the achievable network utilization level is difficult and can vary significantly based on the following key parameters:

- Operating software (e.g. Microsoft® Windows® XP, Microsoft Windows 2000, etc.) and its maintenance level
- Workstation / Server hardware and configuration settings
- Software browser, specifically Internet Explorer®
- Shared workload on the workstation /server
- Transfer file size

Based on lab environment testing and customer experience to date, the achievable network utilization level has varied significantly based on each unique environment. The table below outlines some of the

network options and their corresponding potential transfer rates. These estimates are based on extrapolations from internal testing of some connection options and should be considered as guidelines.

Specifically, FRB testing of Microsoft Windows XP Service Pack 1 using Internet Explorer over a dedicated T1 line could only approach a network utilization level of 30%. Thus, your organization must take great care in assessing achievable network utilization in its specific environment.

Internet Connectivity Available Bandwidth	Potential Transfer Rate Checks/Hour	Potential Transfer Rate Checks/Hour	Potential Transfer Rate Checks/Hour	Potential Transfer Rate Checks/Hour
Network Utilization Level	30%	50%	70%	90%
256 Kbps	1,100	1,800	2,500	3,300
384 Kbps	1,600	2,700	3,800	4,900
512 Kbps	2,200	3,600	5,100	6,600
768 Kbps	3,300	5,500	7,700	9,900
1.544 Mbps	6,600	11,100	15,500	20,000

Above estimates assume an average size check of 25,000 bytes.

Should your organization's ISP service become unavailable, upload or download of ICLs cannot occur unless a contingency location or alternate ISP is available.

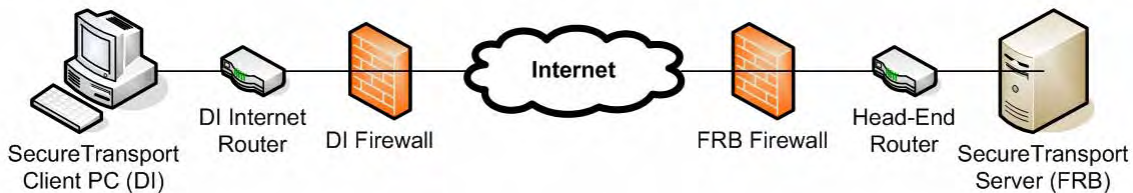
Implementation Considerations When Selecting Option 1

If a sufficient transfer rate cannot be achieved during the desired file transfer window and/or contingency service has not been established, your organization should consider one or all of the following:

- Implementing SecureTransport client software outlined in Option 2
- Implementing additional bandwidth
- Adjustments to the operating environment
- Implementing contingency internet service

Lead time for implementation of such enhancements must be considered in scheduling implementation of Check 21 services.

<p>ICL Transfer Option 2:</p> <p>Customer-Initiated Automated Upload and Download via the Internet Using Tumbleweed SecureTransport Software</p>	<p>Your organization can automate the file upload and download processes through the Internet by purchasing and installing the Tumbleweed SecureTransport client software on your host system. Tumbleweed offers the SecureTransport client for versions of Microsoft Windows, Linux[®], and Solaris[®] operating systems. The SecureTransport client software communicates with the FRB's SecureTransport server software to facilitate file transfers.</p> <p>During the implementation process, a dedicated user will be issued FRB security credentials² in order to facilitate authentication of the SecureTransport client at your organization's location with the SecureTransport server software at the FRB site. Your organization can customize the SecureTransport client settings to automatically upload and download ICLs at designated times. In addition, the SecureTransport client offers mid-file recovery capabilities, which automatically resume file transfers in the event of communication line disruptions.</p>
<p>Security</p>	<p>Files are transferred between FRB and your organization via HTTPS. Data encryption is provided by a mutually authenticated session using FRB issued credentials.</p> <p>The diagram that follows depicts Option 2 for financial institutions:</p>



² More information on FRB security credentials can be found on www.frbservices.org

**Considerations in
Selecting Option 2**

File transfer via the Internet using the Tumbleweed SecureTransport client software is suggested for consideration by organizations with daily check volume of less than 100,000 in either deposits or presentments and those that can consistently transfer files effectively within the following guidelines:

- Total daily transfer time for either all deposit files or all presentment files should be less than 2 hours
- If total daily transfer time for either all deposit files or all presentment files exceeds 2 hours, minimum transfer rate of 3 Mbps must be achieved
- Total daily transfer time for either all deposit files or all presentment files can not exceed 3 hours
- Total number of daily deposit and presentment files from/ to a single customer is less than 400

Single customer is defined as a financial institution or a third party service provider supporting multiple financial institutions.

Those customers that can not achieve the above guidelines must take corrective action to comply with the guidelines or to evaluate Option 3 in order to establish the most effective file transfer process and maximize the ability to meet the desired deadlines.

Your organization can purchase SecureTransport client software directly from Tumbleweed utilizing the on-line portal that has been established for FRB customers at <https://portal1.tumbleweed.com/frstore/TMWDSStore> . The SecureTransport client provides mid-file recovery, which resumes file transfers from the point of communication line disruption. It also provides the ability to automate authentication and the upload/download functions³. The software cost is about \$300 with an annual maintenance fee of about \$50. For more information and firm pricing on this software product please visit the Tumbleweed website at www.tumbleweed.com/products/securetransport/securetransport_client.html.

Your organization must have a sufficient connection to the Internet that can support an effective transfer of its daily check volume at the desired deadlines. Check image files are much larger than most other application data files. A single check, front and back, captured as a black-and-white image, is typically around 25,000 bytes, although it can vary based on the specific check stock. By identifying the number of checks in your organization's files and the desired transfer times, peak transfer rate requirements can be determined.

Your organization must carefully evaluate your Internet connection speed and daily usage patterns. Achievable transfer rates are impacted by many factors, but two that can have a significant influence include available bandwidth and the financial institution's operating environment.

Determining available bandwidth should include the following key

parameters:

- Upload and download bandwidths provided by the internet service provider (ISP) may differ significantly
- Connectivity that is shared by other applications may have different available bandwidth during anticipated transfer times
- Your organization's internal network infrastructure capacity

Determining the impact of your organization's operating environment on the achievable network utilization level is much more difficult and can vary significantly based on the following parameters:

- Operating system (e.g. Microsoft Windows XP, Microsoft Windows 2000, Linux, Solaris, etc.) and its maintenance level
- Workstation / Server hardware and configuration settings
- Software browser, specifically Internet Explorer
- Shared workload on the workstation /server
- Transfer file size

Based on lab environment testing and customer experience to date, the achievable network utilization level has varied significantly based on each unique environment. The table below outlines some of the network options and their corresponding potential transfer rates. These estimates are based on extrapolations from internal testing of some of the connection options and should be considered as guidelines.

The internal testing of Microsoft Windows XP Service Pack 1 using SecureTransport client software over a dedicated T1 line resulted in a network utilization level of about 90%. Your organization must take great care in assessing achievable network utilization in its specific environment.

The following table summarizes the impact different network utilization levels can have on the potential transfer rate of checks for various network bandwidths:

Internet Connectivity Available Bandwidth	Potential Transfer Rate Checks/Hour	Potential Transfer Rate Checks/Hour	Potential Transfer Rate Checks/Hour	Potential Transfer Rate Checks/Hour
Network Utilization Level	30%	50%	70%	90%
256 Kbps	1,100	1,800	2,500	3,300
384 Kbps	1,600	2,700	3,800	4,900
512 Kbps	2,200	3,600	5,100	6,600
768 Kbps	3,300	5,500	7,700	9,900
1.544 Mbps	6,600	11,100	15,500	20,000
2 Mbps	8,600	14,400	20,100	25,900
3 Mbps	12,900	21,600	30,200	38,800

	4 Mbps	17,200	28,800	40,300	51,800
<p>Above estimates assume an average size check of 25,000 bytes.</p> <p>The current FRB security infrastructure limits file transfer time of a particular file to one hour in duration thus consideration must be given to assure effective file transfer.</p> <p>Should your organization's ISP service become unavailable, upload or download of ICLs cannot occur unless a contingency location or alternate ISP is available.</p> <p>Financial institutions that initially selected Option 1 can upgrade to Option 2 at any point.</p>					

<p>Implementation Considerations When Selecting Option 2</p>	<ol style="list-style-type: none"> 1. If a sufficient transfer rate or time can be achieved and contingency service has been established, your organization needs to allocate adequate lead time and resources to obtain, install and set up the SecureTransport client software. 2. If a sufficient transfer rate or time cannot be achieved or contingency service has not been established, your organization should consider additional bandwidth, alternative ISP providers, adjustments to the operating environment and contingency internet service. Lead time for implementation of such enhancements must be considered in scheduling implementation of Check 21 services. 3. The time that files will be available for delivery to FRB or receipt from FRB should be verified prior to setting a scheduled time for automated file upload or download within the SecureTransport client software. 4. FRB will monitor customer transfer time and effective transfer rates on a monthly basis. Those exceeding the guidelines will be notified, and the customer will be requested to provide a corrective action plan within 30 days of notification.
<p>Scripting Considerations with Tumbleweed's SecureTransport Client</p>	<p>Microsoft Windows</p> <p>The SecureTransport client for Microsoft Windows is designed to run with either a graphical user interface or through the DOS command line within the operating system.</p> <p><u>Though the SecureTransport client offers a scheduler function within the graphical user interface, the command line version offers a higher level of control over the operation of the client. A simple command line file upload script can be structured as follows:</u></p> <pre style="text-align: center;"> "C:\Program Files\Tumbleweed\STClient\stclient.exe" "https://<host address>/<junction name>/incoming/" "C:\<your outgoing file directory>*" /hidden /quitWhenDone /root <junction name> /prefNoAskSched/ statusBAT xferStatus.bat /Remote-Site <SITE LABEL> </pre> <p><u>The following is the syntax for a sample download script:</u></p> <pre style="text-align: center;"> "C:\Program Files\Tumbleweed\STClient\stclient.exe" "https://<host address>/<junction name>/outgoing/" "C:\<your incoming file directory>*" /hidden /quitWhenDone /root <junction name> /prefNoAskSched/ statusBAT xferStatus.bat /Remote-Site <SITE LABEL> </pre> <p><u>Variations of these scripts can be run from a Windows-based scheduler program to upload and download files between the customer network and the Federal Reserve Bank along with custom processing scripts written by the customer. Please contact Tumbleweed for support on</u></p>

custom scripting using the SecureTransport client for Microsoft Windows.

Linux and Solaris

The SecureTransport client for UNIX[®]-based systems such as various distributions of Linux and Solaris is designed to run as a command-line application similar to the “ftp” command with custom functionality for use with a SecureTransport environment. The Linux and Solaris version has additional features not found in the Windows version of the SecureTransport client such as directory listing.

The SecureTransport client upload command for Linux and Solaris can be executed as follows:

```
fdx -i -A -u  
    /<your file directory>/*  
    https://<host address>/<junction name>/incoming/
```

The following is the syntax for a sample download script:

```
fdx -i -A -d  
    https://<host address>/<junction name>/incoming/*  
    /<your file directory>/
```

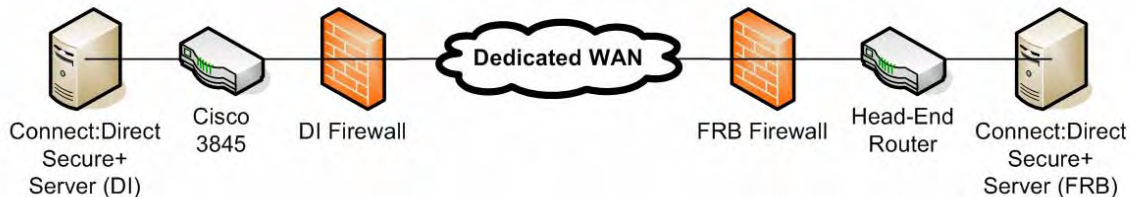
The Linux and Solaris versions of the SecureTransport client do not have a scheduler feature; however, customers may create a CRON job within the Linux and Solaris-based operating systems for regularly scheduled execution. Please contact Tumbleweed for support on custom scripting using the SecureTransport client for Linux and Solaris.

Scheduling and Execution of Custom Scripts

The Federal Reserve Bank requires at least a 15 minute script interval for interrogating the system for new FedReceipt files for download.

For customers with volumes of greater than 45,000 checks per day, there may be added benefits in using a Linux or Solaris platform and client over the Microsoft Windows client for a higher degree of script customization and efficiency in file retrieval.

<p>ICL Transfer Option 3:</p> <p>Upload and Download via Direct Network Connection Using Sterling Commerce Connect:Direct Secure+ Software</p>	<p>Your organization can initiate upload and download of ICLs automatically or manually through a direct connection to the FRB network using Sterling Commerce Connect:Direct Secure+ software installed on its host systems. To initiate ICL transfer, your organization's Connect:Direct Secure+ software authenticates with the FRB's Connect:Direct Secure+ software using FRB-issued credentials⁴. Connect:Direct Secure+ software allows your organization to schedule automated transfers of files to the FRB or to manually control such transfers. In the event of a communication line disruption, the software also provides the ability to resume a file transfer from the point of disruption rather than from the beginning, thus minimizing the impact of communication problems on file transfers.</p> <p>If your organization is a FedReceipt customer, ICLs will be delivered to you automatically as soon as they become available. This process follows the same authentication process as above, except the FRB's Connect:Direct Secure+ software initiates the file transfer session. In addition, your organization can choose to further customize the file transfer process by adding run tasks functions.</p>
<p>Security</p>	<p>The direct network connection uses a private IP network. This network uses Multi Protocol Label Switching (MPLS) technology and provides private groupings in order to segment traffic to discrete areas of the network. Security is provided through point-to-point router linkages with IPSec, VPN tunneling and a dedicated WAN connection.</p> <p>The network provides the ability to deploy connections ranging from T1 (1.5Mbps) to DS3 (10Mbps-45Mbps) to OC3 (35 Mbps -155Mbps). As part of the direct network connection service, the FRB provides and maintains the router and circuits for specified customer locations. Table 1 below provides an example of components that may be included in a direct network connection deployment. Your organization is responsible for its firewall and server infrastructure including the Connect:Direct Secure+ software to support ICL transfer.</p> <p>The diagram that follows depicts Option 3 for financial institutions:</p>



**Considerations in
Selecting Option 3**

File transfer via direct network connection is suggested if your organization has a daily volume exceeding 100,000 checks and those that can not meet the transfer guidelines for Internet (Option2). This would establish an effective file transfer process that maximizes the ability to meet the desired deadlines.

Your organization must provide the host system running Sterling Commerce Connect:Direct Secure+ software. If your organization is not currently utilizing Connect:Direct or Secure+ software, you should contact Sterling Commerce for the associated costs since they can vary based on system configurations.

Assessing bandwidth requirements is very important in order to accomplish a desired transfer rate of checks. Check image files are much larger than most other application data files. A single check, front and back, captured as a black-and-white image, is typically around 25,000 bytes, although it can vary based on the specific check stock. By identifying the number of checks in your organization's files and the desired transfer times, peak transfer rate requirements can be determined.

The following table outlines the network options and their corresponding potential transfer rates. These estimates are based on extrapolations from internal testing of some of the connection options and should be considered as guidelines. There are many factors that can affect the achievable transfer rate including your organization's internal network infrastructure and type of platform in use (e.g. hardware, operating system, software).


Line Size	Potential Hourly Transfer Rate	Line Size	Potential Hourly Transfer Rate
T1 - 1.5Mbps	22,000	OC3 - 35Mbps	504,000
4 T1 - 6Mbps	88,000	OC3 - 50Mbps	720,000
DS3 - 10Mbps	144,000	OC3 - 60Mbps	864,000
DS3 - 15Mbps	216,000	OC3 - 75Mbps	1,080,000
DS3 - 25Mbps	360,000	OC3 - 100Mbps	1,440,000
DS3 - 35Mbps	504,000	OC3 - 125Mbps	1,800,000
DS3 - 45Mbps	648,000	OC3 - 155Mbps	2,232,000

Above estimates assume an average size check of 25,000 bytes.

The direct network connection is dedicated to exchanging Check 21 files with the FRB and cannot be used for other Federal Reserve Financial Services. However, a customer may leverage Connect:Direct software for other applications or connections.

The cost of the direct connection varies by location and increases as bandwidth increases. The FRB can provide pricing information for a particular line configuration after assessing the location with the

	<p>network provider. The monthly charges include appropriate router, specific line configuration and corresponding annual maintenance and support. To price a network connection, please contact your FRB Account Executive.</p> <p>Lead times for implementing a new circuit for the direct network connection can vary from 60 to 90 business days. In some cases, the lead time may be even longer based on specific site considerations. Upgrades to different line types (e.g. T1 to DS3, DS3 to OC3) require the same implementation lead time. Lead times for increasing bandwidth within a line type (e.g. DS3 10 Mbps to DS3 20 Mbps) are typically two to four weeks from the commitment date as long as the FRB has sufficient capacity.</p> <p>Your organization needs to consider connectivity needs to support contingency plans. These plans may require a direct network connection to a contingency location.</p> <p>Your organization must agree to perform server authentication using Connect:Direct Secure+ software and an FRB-issued certificate. (FRB authentication of your organization’s server can not be completed using certificates issued by others.)</p> <p>Due to the significant effort and costs involved, a minimum usage commitment of 12 months is required for the direct network connection.</p> <p>Financial institutions that initially select other connectivity options may deploy Option 3 at any point in the future.</p>
<p><i>Implementation Considerations When Selecting Option 3</i></p>	<ol style="list-style-type: none"> 1. Bandwidth and location assessments need to occur as early in the process as possible in order to determine a preliminary schedule for deployment. 2. If the financial institution is not currently using Connect:Direct Secure+ software, the financial institution needs to allocate adequate lead time and resources to obtain, install and set up the software. 3. Depending on the network size, a customer can set up multiple concurrent Connect:Direct sessions to maximize its throughput: <ul style="list-style-type: none"> - Multiple T1s 5-10 concurrent sessions - DS 3 10-20 concurrent sessions - OC 3 up to 32 concurrent sessions 4. Circuit installation lead time needs to be considered in scheduling deployment of Check 21 services. 5. Internet connectivity can be utilized to support initial testing and lower volume production while the Direct Network Connection is being installed.

<p>Table 1: Example of Direct Network Connection Component List</p>	<p>Below is an example of a component that may be used to implement a direct network connection at your organization. Specific components will vary based on connection type. The role of each component can be reviewed with FR technical staff during the implementation process.</p>
<p>WAN Router Information</p>	<p>Cisco 3845 series router Information</p>  <p>This router features:</p> <ul style="list-style-type: none"> • Two Gigabit Ethernet ports • One set DS-3 RX/TX coaxial connections with DS-3 Card • One console port, One auxiliary port • Dimensions (h x w x d): 5.25 x 17.25 x 16 in. (133.4 x 438.2 x 406.4 mm), Weight: 45 LBS • 3-RU height • Redundant PSU, 440W maximum power distribution

Summary of Connectivity Options for ICL Transfer

The following table provides a summary of the key features and differences of the three connectivity options:

Feature / Characteristic	Option 1 Internet with FedLine Web	Option 2 Internet with SecureTransport Client	Option 3 Direct Network Connection
Daily volume target	< 2,000 checks	< 100,000 checks	>100,000 checks
Total daily transfer time	<20 minutes	< 2 hours in either deposits or presentments; can not exceed 3 hours	N/A
Transfer rate	Sufficient to meet the transfer time	>3 Mbps if total transfer time in either deposits or presentments is > 2 hours	Based on network size elected
Daily number of files	Few	<400 files for both deposits and presentments	Unlimited
File transfer utility	HTTP	SecureTransport client from Tumbleweed	Connect:Direct Secure+ from Sterling Commerce
Network use	Shared or dedicated	Shared or dedicated	Dedicated to FRB Check 21-enabled services
Security	<ul style="list-style-type: none"> - User authenticated via FRB issued credentials - File encryption by mutually authenticated session 	<ul style="list-style-type: none"> - Client authenticated via FRB issued credentials, - File encryption by mutually authenticated session 	<ul style="list-style-type: none"> - Server authenticated via Secure Plus using FRB issued credentials - Point to point router link with IPSec, VPN tunneling and triple DES encryption - Private IP network using MPLS technology
Line interruption recovery	Requires restart of file transfer in case of line disruption	Resumes at point of line disruption (i.e. mid-file recovery)	Resumes at point of disruption (i.e. mid-file recovery)
File transfer options	User initiated <ul style="list-style-type: none"> - File 'Push' to upload - File 'Pull' to download 	User initiated or scripted <ul style="list-style-type: none"> - File 'Push' to upload - File 'Pull' to download 	Automated <ul style="list-style-type: none"> - File 'Push' to upload and download