June 7, 2017

Dear Valued Client,

In order to continue to ensure a high level of data security during the file transfer process, TSI will be updating the SSH host key which helps identify TSI's server and enables encryption (similar to the certificates used for HTTPS web pages).

The change will require you to accept the new SSH Host Key which can be accomplished in multiple ways depending on the application/software that you use to access our SFTP server and depending on whether you have automated scripting set up for the file transfer process.

Please review the information below and be prepared to verify and accept the new SSH Host Key to ensure that we are able to continue to transmit data securely. The change will be made on July 11th 2017; therefore *it is imperative that this communication is provided to the technical contact person within your organization who is responsible for the file transfer process as quickly as possible*.

When connecting to our clientftp.tsico.com server originally, you would have accepted our host key. It might have identified itself with either of the following strings of characters (often referred to as a "fingerprint"):

0d:af:a8:b0:1c:1c:6d:7b:63:60:a9:f2:8b:6f:71:ae

xovan-pikos-momas-cutyr-kekun-dagom-piget-bapeb-volyn-nuzeg-koxyx (DSA)

Effective on 07/11/17 when we roll out the new host key, your SSH/SFTP software will likely display an error that the host key isn't known, or display a message indicating an existing key was already saved for this host and the new one doesn't match (please refer to the bottom of this communication for examples). The key identification strings, also called the "fingerprint" for the new host key should be one of these strings:

- 84:ab:2d:3e:7d:03:76:44:75:7f:38:d2:4f:6e:7e:19
- D5 74 DA CE F3 32 90 79 9F 86 3E 6F 5D 6A A9 45 E8 CA 16 0E (RSA)
- D574 DACE F332 9079 9F86 3E6F 5D6A A945 E8CA 160E (RSA)
- d574dacef33290799f863e6f5d6aa945e8ca160e (RSA)
- D574DACEF33290799F863E6F5D6AA945E8CA160E (RSA)
- xuhel-gekas-vosof-degol-nulam-kozuk-zolik-pepeg-hipis-pohib-voxax (RSA)
- XUHEL-GEKAS-VOSOF-DEGOL-NULAM-KOZUK-ZOLIK-PEPEG-HIPIS-POHIB-VOXAX (RSA)

If the new fingerprint displayed by your application matches one of these strings, you may accept the key and continue with the connection.

500 Virginia Drive
Suite 514
Fort Washington, PA
19034-2707
www.tsico.com

Accounts Receivable Management
Collections
Loan Servicing
Billing & Payments
Analytics

We get cash flowing

If the fingerprint displayed by your application DOES NOT match one of these strings, DO NOT continue with the connection. Please capture a screen shot of the warning message and email it to us at cs@tsico.com, and we will evaluate. If your application is merely using an alternate method of displaying the fingerprint, we should be able to verify this and send you confirmation to continue.

The TSI team remains focused on serving your needs and keeping your data secure. If you have questions about your account and/or this change, please e-mail TSI Client Services at cs@tsico.com. Please include “SFTP SSH Host Key <your company name>” in the subject line.

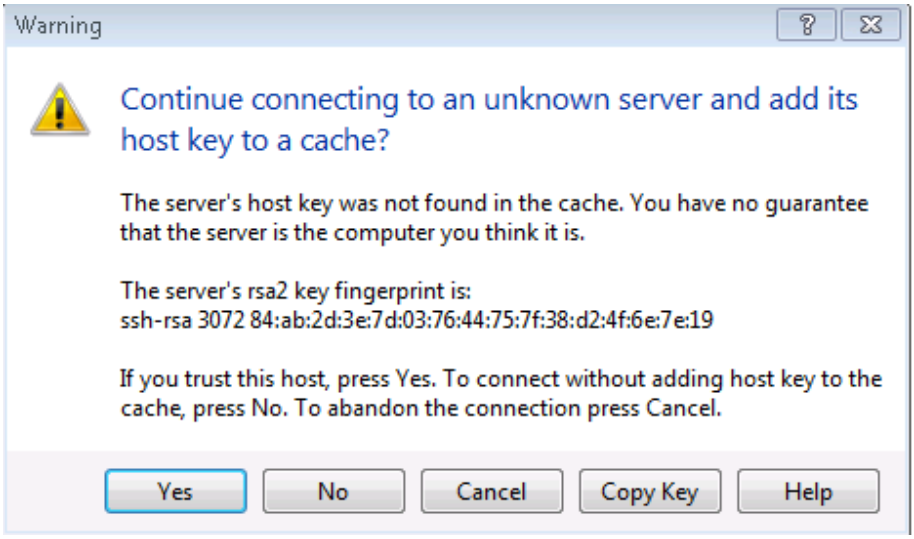
On behalf of the leadership teams at TSI, we appreciate your business and the privilege to serve your customers.

Sincerely,

TSI Client Services & IT

NOTE: While not all applications will display the same, here are several examples to help show you what you might expect to see.

WinSCP example:



(See additional examples on next page.)

PuTTY's psftp example:

```
C:\Program Files\PuTTY>psftp clientftp2.tsi-ad.com
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 3072 84:ab:2d:3e:7d:03:76:44:75:7f:38:d2:4f:6e:7e:19
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n)
```

Linux command-line sftp example:

```
$ sftp clientftp2.tsi-ad.com
Connecting to clientftp2.tsi-ad.com...
WARNING: DSA key found for host clientftp2.tsi-ad.com
in /home/rgreene/.ssh/known_hosts:580
DSA key fingerprint 0d:af:a8:b0:1c:1c:6d:7b:63:60:a9:f2:8b:6f:71:ae.
+--[ DSA 2048]----+
|                 |
|                 |
|        .        |
|   . .   +       |
|  . *   S o      |
| ..=.o . .       |
|. =+. = .        |
| =.+.+ .         |
|.oEo.            |
+-----------------+

The authenticity of host 'clientftp2.tsi-ad.com (10.40.212.17)' can't be establi
shed
but keys of different type are already known for this host.
RSA key fingerprint is 84:ab:2d:3e:7d:03:76:44:75:7f:38:d2:4f:6e:7e:19.
Are you sure you want to continue connecting (yes/no)?
```