Security Advisory:
PCI v3.2 Requirements-Changes to Encryption Protocols

This notice is a reminder that BridgePay will be migrating it's production systems to use TLS 1.2 in 2018. BridgePay systems currently support TLSv1, TLSv1.1 and TLSv1.2. However, after June 30, 2018, BridgePay production systems will no longer support TLSv1 or TLSv1.1.

In order to facilitate testing, BridgePay will be migrating all of its test systems to TLS 1.2 on May 1, 2017.

What systems are affected by this announcement?
Any system that makes an encrypted connection to BridgePay test systems. This includes web browsers, terminals and direct API integrations.

Which Test Sites are affected?

https://boardingstage.itstgate.com
https://cpgtest.cynergydata.com
https://gatewaystage.itstgate.com
https://giftlinkstage.itstgate.com
https://securedecrypt.bridgepaynetsecuretest.com
https://staging.redfinnet.com
https://www.bridgepaynetsecuretest.com
https://www.mybridgepaytest.com
https://www.sandboxtesting.net

Will the change on May 1, 2017 affect production transactions?
No. Production transactions and sites will not be affected. Only test systems will be affected.

I connect with a web-browser. Am I affected?
Modern web-browsers such as Microsoft Edge, Microsoft Internet Explorer, FireFox and Chrome support TLS 1.2. Consult your IT department to ensure your system is configured correctly. Minimum required versions of some popular client software are: IE 11, FireFox 27, Chrome 30, Opera 17, Safari 7, Android 4.4 and JAVA 8. While JAVA 7 can be configured to use TLS 1.2, JAVA 8 is recommended.

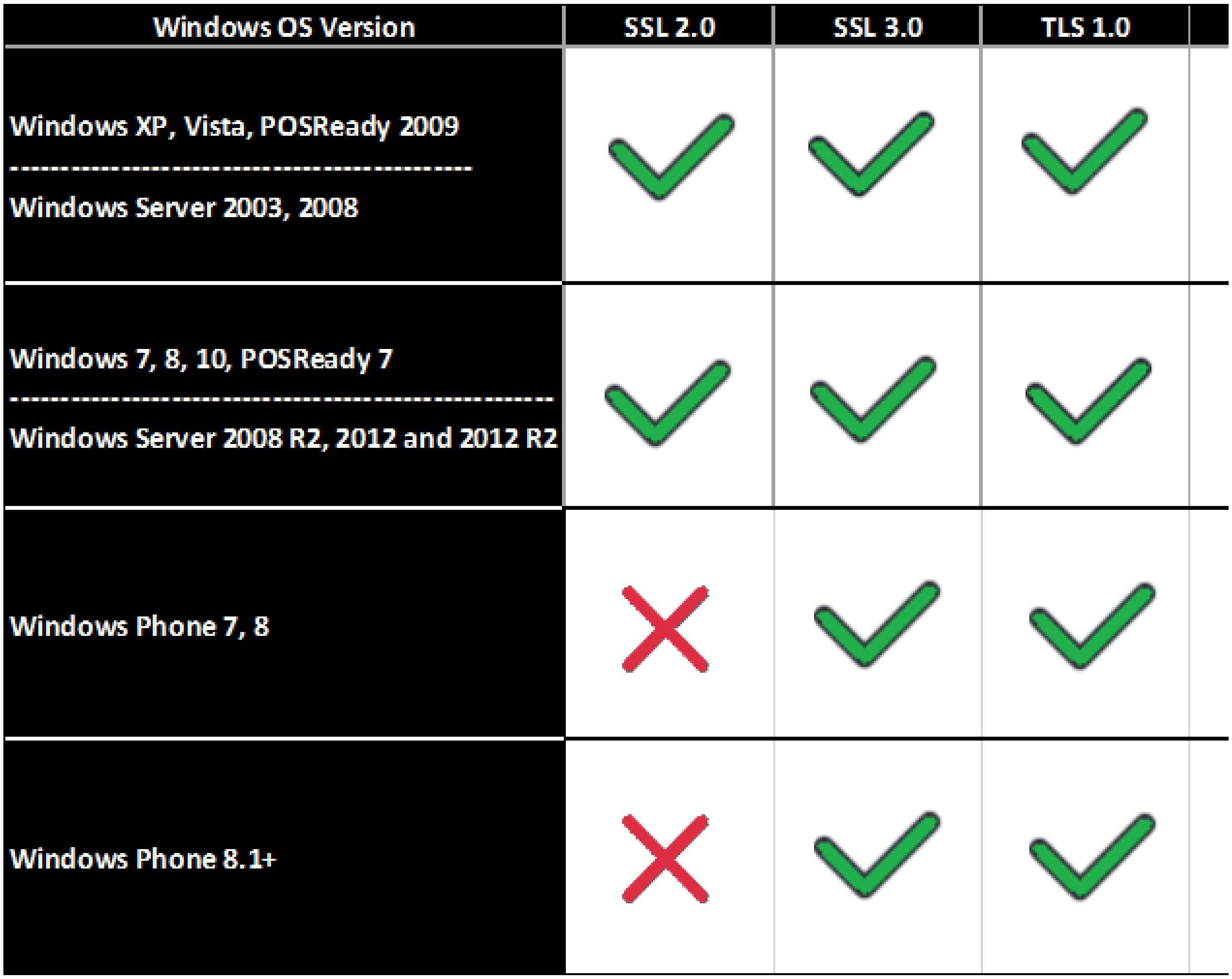
Who should I contact if my terminal needs to be upgraded to use TLS 1.2?
If your terminal does not support the TLS 1.2 protocol, contact your terminal provider for an upgrade.

What Encryption Ciphers are supported?

Modern web-browsers support the latest encryption ciphers under TLS 1.2. For terminal configuration, contact your terminal provider for a list of ciphers the terminal supports. BridgePay will be supporting the cipher list as described in National Institute of Standards and Technology Special Publication (NIST SP 800-52 rev 1).

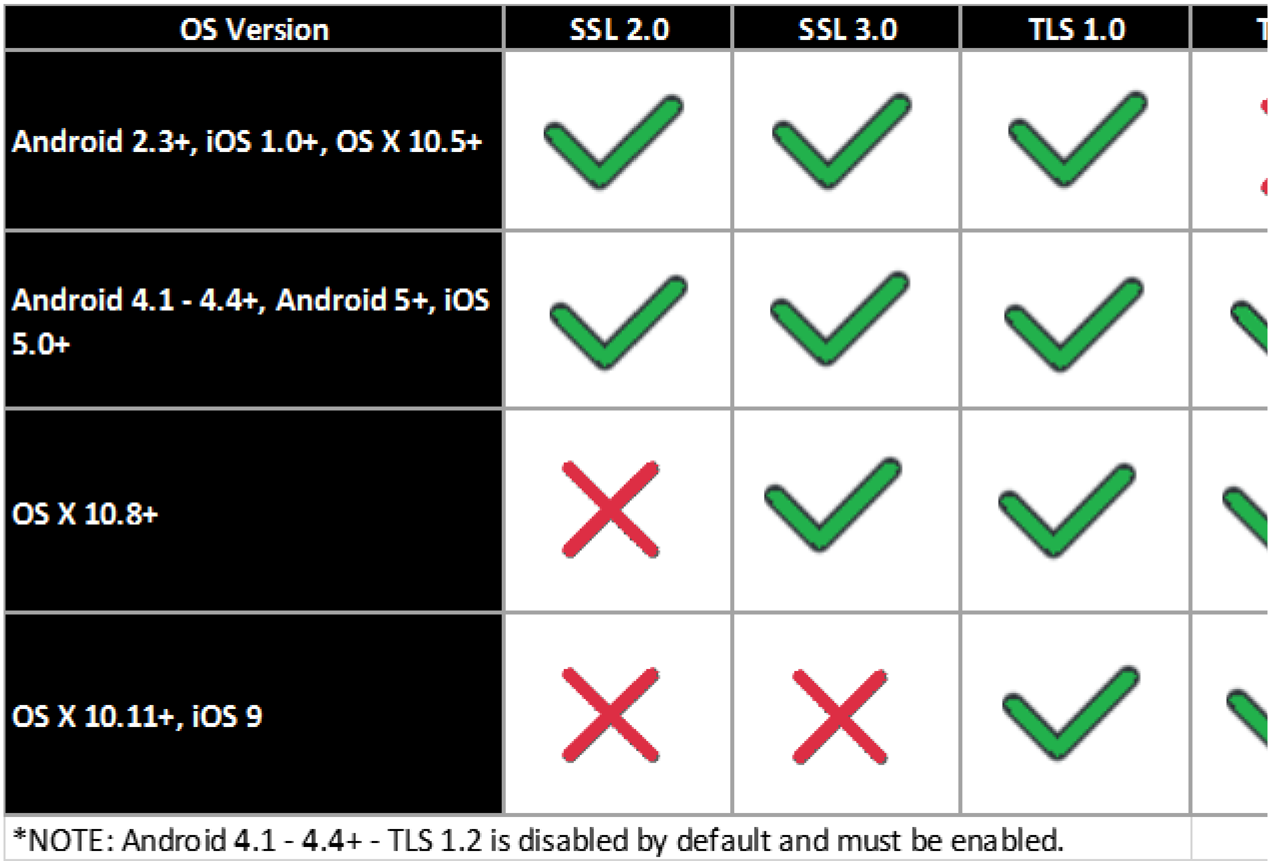
What Windows Operating System (OS) supports TLS 1.2?

The table below describes which OS versions support which version of TLS.



Windows OS Version	SSL 2.0	SSL 3.0	TLS 1.0
Windows XP, Vista, POSReady 2009 --- Windows Server 2003, 2008	✓	✓	✓
Windows 7, 8, 10, POSReady 7 -- Windows Server 2008 R2, 2012 and 2012 R2	✓	✓	✓
Windows Phone 7, 8	✗	✓	✓
Windows Phone 8.1+	✗	✓	✓

What are other popular Operating Systems (OS) supports TLS 1.2?



OS Version	SSL 2.0	SSL 3.0	TLS 1.0	T
Android 2.3+, iOS 1.0+, OS X 10.5+	✓	✓	✓	✗
Android 4.1 - 4.4+, Android 5+, iOS 5.0+	✓	✓	✓	✓
OS X 10.8+	✗	✓	✓	✓
OS X 10.11+, iOS 9	✗	✗	✓	✓
*NOTE: Android 4.1 - 4.4+ - TLS 1.2 is disabled by default and must be enabled.				

Below are some links that may help with understanding these changes:
PCI Security Standards - Migrating from SSL
PCI Security Standards - Bulletin on Migrating from SSL and Early TLS
PCI Security Standards - Summary of Changes
NIST Special Publication
Comparison of TLS Implementations
Transport Layer Security Web Browsers

Thank you,
Gateway Support
gateway.support@bridgepaynetwork.com

[redacted]