

## **BIG PCI CHANGES BROUGHT ON BY POODLE**

SSL encryption is a standard encryption method used for decades. A vulnerability named POODLE has been detected within SSL and is no longer PCI compliant. POODLE (Padding Oracle on Downgraded Legacy Encryption) is a vulnerability in SSL that could allow a hacker to extract data from secure online connections.

Why should you care? Well, there could be a loss of confidential data that allows an attacker to decrypt sensitive information on your systems.

According to the [PCI Standards Council Blog](#), the Payment Card Industry Standards Council (PCI SSC) is extending the migration completion date to June 30, 2018, for transitioning from SSL AND TLS 1.0 to a secure version of TLS (currently v1.1 or higher).

The new date of June 2018 (with some deadlines as soon as this summer) offers additional time to migrate to more secure protocols, but waiting is not recommended.

The existence of the POODLE and Heartbleed exploits, among others, prove that anyone using SSL and before TLS risks a breach. To view the PCI Standard Council's Q & A regarding compliance visit the [PCI Standards Council Bulletin on migrating from SSL](#).

### **So How Do You Keep Your POS System Secure?**

Once the deadline is up, the credit card processing functionality of any non-compliant equipment will cease. This is an industry-wide requirement. Most legacy POS systems are vulnerable and will need to be upgraded before the deadline.

To remain PCI compliant, merchants, in some cases, will need to update software, operating systems, and/or hardware. Merchants who refuse to upgrade their system will not be able to process credit cards once the deadline is met.

**Harbortouch** has gotten out ahead of the potential POODLE SSL vulnerability disruption and is fully PCI compliant, but most POS companies are just starting to become aware of this issue and it is likely that many of them will be severely impacted in the months to come.

First Data and other large processors were recently hit by a similar disruption over the holidays caused by the expiration of a security certificate called SHA-1. Harbortouch was unaffected since they were able to update all the certificates to the new SHA-2 requirement through extensive conversion efforts. The POODLE SSL issue is going to be exponentially more severe than the SHA-1 certificate since virtually all POS systems rely on SSL.

Give us a call to see how we can help...

<https://lendingcapital.net>