Re: Risk Mitigation and Migration Plan for PCI DSS 3.1 Requirements

Please accept this as the Risk Mitigation and Migration Plan for PCI DSS 3.1 for **COMPANY NAME**.

1. Where are SSL/TLS 1.0 currently used in your environment?

We use TLS 1.0 on the customer login page and customer order page of our website.

2. How are you mitigating risks with SSL/TLS 1.0?

We have disabled SSLv3 entirely, and the vast majority of our customers use browsers that support TLS 1.1 or 1.2. We use TLS_FALLBACK_SCSV to prevent "downgrade attacks" that could force these browsers to use TLS 1.0.

This means that none of our visitors use SSLv3, and only a small number use TLS 1.0. However, disabling TLS 1.0 without sufficient notice would cause these customers to be unable to use our website. We will encourage these customers to upgrade their browsers as soon as possible.

3. How are you monitoring for new vulnerabilities associated with SSL/TLS 1.0?

The engineers at our hosting company monitor relevant security-focused mailing lists, including those from Debian Linux security, Sucuri, and OpenSSL.

4. How are you ensuring that SSL/TLS 1.0 are not introduced into your cardholder data environment? (Meaning, how can you verify that new or upgraded systems connected to your cardholder data environment don't contain SSL/TLS 1.0?)

Our hosting company, which is responsible for the encryption methods on our server, has verified that they will review all new software to ensure nothing is introduced that uses SSLv3 or TLS 1.0.

5. When will your migration plan from SSL/TLS1.0 be completed?

This will be completed by June 30, 2018.