Cover Letter for WebTrust Audit Covering
December 1, 2015 through November 30, 2016

March 31, 2017

Symantec's WebTrust audit reports have been issued by KPMG for the period December 1, 2015 through November 30, 2016. Electronic copies of this audit's reports are located at: https://www.symantec.com/about/legal/repository.jsp. This year's WebTrust audit reports were divided into the first half of the year and the second half of the year. Below are findings from the second half report.

Specifically, there are no negative qualifications in our WebTrust for Certificate Authorities report and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL reports for the second half. The SSL Baseline reports do contain qualifications, as described below.

Observations from WebTrust Audit (June 16, 2016 – November 30, 2016):

1. Formal Documentation of Vulnerabilities Exceptions: It was noted that there were inconsistencies in documentation for dispositions of identified vulnerabilities that did not require remediation. We have implemented documentation improvements to our vulnerability management program.
2. Lack of Internal Scans and Penetration Testing: It was noted that quarterly external scanning was in place but internal scanning was not occurring for one of Symantec's international locations. The audit also found that penetration testing was missing for this international location. All issues have now been addressed - we now scan both internally and externally and penetration testing is in progress and should conclude shortly.
3. (Previously disclosed and resolved) Internal Server Names: As was required and documented, all still valid internal server name certificates needed to be revoked by October 1, 2016; however, a total of 10 certificates were missed in the revocation process performed before the deadline. We immediately revoked these certificates and disclosed this event on the Mozilla public forum on January 11, 2017 and January 20, 2017 at https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/00gci6NII9Y.
4. (Previously disclosed) Certificate Issuance with a sequential serial number for a Critical Customer Infrastructure Issue: It was noted that a customer with a critical infrastructure issue requested issuance of a certificate under a specific issuing CA operated on a deprecated platform that only supported sequential serial numbers, in violation of CA/B Forum Baseline Requirements section 7.1. Due to the criticality of the issue and the significant financial impact to the customer of not doing so, we issued a replacement certificate with a limited validity period of three months for remediation. We disclosed this event on the CA/Browser Forum public mailing list on November 27, 2016 at https://cabforum.org/pipermail/public/2016-November/008989.html
5. Inclusion of an International Location in Audits: It was noted that in audits previous to this WebTrust audit, an international location had not been included in the sampling. Once identified, this location was included in the audit sample and is part of this WebTrust audit.

You may note that this audit did not include a review of the recent issue in connection with one of Symantec's former Registration Authorities (RA). These mis-issuances were discovered after the time period covered by our current WebTrust audit reports, and would fall within the audit for our RA partner had we continued the program. Instead, we are revalidating all of this partners' active certificates, and reviewing all of those issued by all other RA partners. This review and revalidation will be in the scope of our next audit.

Concurrent with this audit, we have continued to improve and accelerate enhancements to our processes, policies, and controls. We are exploring and will implement methods to keep track of our progress and provide transparency to the broader CA ecosystem and browser community more frequently.

Symantec Corporation

Roxane Divol
EVP and GM, Website Security
