

## Report of Independent Accountants

To the Management of Web.com Group, Inc.

We have been engaged to report on Network Solutions, LLC's ("Network Solutions," a wholly owned subsidiary of Web.com) operation of its SSL Certification Authority (CA) services at the Herndon, Virginia, United States; Clifton, New Jersey, United States; Weehawken, New Jersey, United States; Bradford, England, United Kingdom; and Manchester, England, United Kingdom locations, regarding whether during the period from April 1, 2014 through March 31, 2015, Web.com:

- Disclosed its SSL certificate life cycle management business practices in its [Certification Practice Statement](#), including its commitment to provide SSL certificates in conformity with the applicable CA/Browser Forum Guidelines on the Network Solutions website.
- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and SSL certificates it managed is established and protected throughout their life cycles; and
  - SSL subscriber information was properly collected, authenticated (for the registration activities performed by Network Solutions) and verified.
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.
- Maintained effective controls to provide reasonable assurance that it met the Network and Certificate System Security Requirements set forth by the CA/Browser Forum

based on the [WebTrust<sup>SM/TM</sup> Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0](#).

These disclosures and controls are the responsibility of Web.com's management. Our responsibility is to express an opinion based on our examination.

Network Solutions makes use of external registration authorities for specific subscriber registration activities as disclosed in Network Solutions' business practice disclosures. Our examination did not extend to the controls exercised by the external registration authorities.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of Network Solutions' key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4)

performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Network Solutions and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, Network Solutions' ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In performing our engagement, we noted the following matter that prevented certain SSL Baseline Audit Criteria from being met during the audit period from April 1, 2014 through March 31, 2015: Principle 3, Criterion 2: Network Solutions did not perform a formal risk assessment during the audit period. As a result, Principle 3, Criterion 2 *The CA performs a risk assessment at least annually that: Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats*, was not met.

In our opinion, except for the matter described in the previous paragraph, during the period April 1, 2014 through March 31, 2015, Network Solutions, in all material respects

- Disclosed its SSL certificate life cycle management business practices in its [Certification Practice Statement, including](#) its commitment to provide SSL certificates in conformity with the applicable CA/Browser Forum Guidelines on the Network Solutions website.
- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and SSL certificates it managed is established and protected throughout their life cycles; and
  - SSL subscriber information was properly collected, authenticated (for the registration activities performed by Network Solutions) and verified.
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.
- Maintained effective controls to provide reasonable assurance that it met the Network and Certificate System Security Requirements set forth by the CA/Browser Forum

based on the [WebTrust<sup>SM/TM</sup> Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0.](#)



This report does not include any representation as to the quality of Network Solutions' certification services beyond those covered by the [WebTrust<sup>SM/TM</sup> Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0](#) criteria, or the suitability of any of Network Solutions' services for any customer's intended purpose.

*Ernst & Young LLP*

July 29, 2015