Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 South Hanley Road, Suite 800
St. Louis, MO 63105

INDEPENDENT ACCOUNTANT'S REPORT

To the Management of Visa U.S.A. Inc. ("Visa"):

We have examined Visa's certification authority ("CA") operations at Highlands Ranch, Colorado and Ashburn, Virginia, Visa's disclosure of its SSL certificate life cycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Visa repository, the provision of such services in accordance with its disclosed practices, and the design of its controls over key and SSL certificate integrity, over the authenticity and confidentiality of SSL subscriber and relying party information, over continuity of key and SSL certificate life cycle management operations, and over development, maintenance, and operation of CA systems integrity, and over meeting the network and certificate system security requirements set forth by the CA/Browser Forum, throughout the period April 1, 2016 to March 31, 2017 for its root and issuing CAs, collectively referred to as Visa eCommerce CAs, listed in Appendix A, in scope for SSL Baseline Requirements and Network Security Requirements.

These disclosures and controls are the responsibility of Visa's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0, based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of Visa's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Visa's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 Visa 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, Visa's 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.

We noted the following matters that resulted in a modification of our opinion.

Impacted WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security		Control Deficiency Noted
2 - 2.1	The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following: • Issuer Information (See SSL Baseline Requirements Section 9.1) • Subject Information (See SSL Baseline Requirements Section 9.2) • Certificate Policy Identification (See SSL Baseline Requirements Section 9.3) • Validity Period (See SSL Baseline Requirements Section 9.4) • Subscriber Public Key (See SSL Baseline Requirements Section 9.5) • Certificate Serial Number (See SSL Baseline Requirements Section 9.6) • Additional Technical Requirements (See SSL Baseline Requirements Section 9.7) - Appendix A - Cryptographic Algorithm and Key Requirements - Appendix B - Certificate Extensions. (See SSL Baseline Requirements Section 9)	Extended key usage field required under section 7.1.2.3 of the Baseline Requirements was omitted from a selection of certificates issued.
2 - 5.3	The CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: • The Subscriber requests in writing that the CA revoke the Certificate; • The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; • The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also See SSL Baseline Requirements Section 13.1.5); • The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement; • The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or	We were unable to obtain evidence to verify the revocation was completed within the 24 hour requirement for a selection of revoked certificates.

	the Domain Name Registrant has failed to renew the Domain Name); • The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; • The CA is made aware of a material change in the information contained in the Certificate; • The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; • The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; • The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; • The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; • The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; • Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or • The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time). (See SSL Baseline Requirements Section 13.1.5)	
2 - 4.1 2 - 4.2	The CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate. (SSL Baseline Requirements Section 11.1) The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements: • Identity (SSL Baseline Requirements Section 3.2.2.1) • DBA/Trade name (SSL Baseline Requirements Section 3.2.2.2) • Authenticity of Certificate Request (SSL Baseline Requirements Section 3.2.5) • Verification of Individual Applicant (SSL Baseline Requirements Section 3.2.3) • Verification of Country (SSL Baseline Requirements Section	We were unable to obtain evidence of the domain validation documentation for a certificate issued.

	3.2.2.3) 2 - 4.3 The CA maintains controls and procedures to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification. (See SSL Baseline Requirements Section 11.2)	

This caused the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Criterion outlined above to not be met.

In our opinion, except for the effect of the matters discussed in the preceding paragraph, throughout the period April 1, 2016 to March 31, 2017, in all material respects, Visa has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Visa Public Key Infrastructure Certification Practice Statement, Version 3.1, Effective March 31, 2017;
  - Visa Public Key Infrastructure Certification Practice Statement, Version 3.0, Effective March 3, 2016;
  - Visa Public Key Infrastructure Certificate Policy, Version 3.1, Effective March 31, 2017; and
  - Visa Public Key Infrastructure Certificate Policy, Version 3.0, Effective March 3, 2016including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Visa repository, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust 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 Visa's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0, nor the suitability of any of Visa's services for any customer's intended purpose.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
July 26, 2017

Visa U.S.A. Inc. Management's Assertion

Visa U.S.A. Inc. ("Visa") operates the Certification Authority ("CA") known as the root and issuing CAs, collectively referred to as Visa eCommerce CAs, listed in Appendix A in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

Visa management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL CA services at Highlands Ranch, Colorado and Ashburn, Virginia, throughout the period April 1, 2016 to March 31 2017, Visa has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Visa Public Key Infrastructure Certification Practice Statement, Version 3.1, Effective March 31, 2017;
  - Visa Public Key Infrastructure Certification Practice Statement, Version 3.0, Effective March 3, 2016;
  - Visa Public Key Infrastructure Certificate Policy, Version 3.1, Effective March 31, 2017; and
  - Visa Public Key Infrastructure Certificate Policy, Version 3.0, Effective March 3, 2016,

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Visa repository, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum based on the

WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security, Version 2.0, except for the effects of the matters noted below:

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		Control Deficiency Noted	Management Response
2 - 2.1	The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following: • Issuer Information (See SSL Baseline Requirements Section 9.1) • Subject Information (See SSL Baseline Requirements Section 9.2) • Certificate Policy Identification (See SSL Baseline Requirements Section 9.3) • Validity Period (See SSL Baseline Requirements Section 9.4) • Subscriber Public Key (See SSL Baseline Requirements Section 9.5) • Certificate Serial Number (See SSL Baseline Requirements Section 9.6) • Additional Technical Requirements (See SSL Baseline Requirements Section 9.7) - Appendix A - Cryptographic Algorithm and Key Requirements - Appendix B - Certificate Extensions. (See SSL Baseline Requirements Section 9)	Extended key usage field required under section 7.1.2.3 of the Baseline Requirements was omitted from a selection of certificates issued.	Visa notes the Extended Key Usage field required under section 7.1.2.3 of the Baseline Requirements has been subsequently integrated into all certificate profiles for Information Delivery and eCommerce certificates. Management notes that the issue has been remediated.
2 - 5.3	The CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: • The Subscriber requests in writing that the CA revoke the Certificate; • The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; • The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also See SSL Baseline Requirements Section 13.1.5); • The CA is made aware that a Subscriber	We were unable to obtain evidence to verify the revocation was completed within the 24 hour requirement for a selection of revoked certificates.	Visa notes a plan to standardize and establish consistency across all revocation requests (including the 24 hour revocation requirement), approvals and validation evidence to include our internal certificate requests, is in progress. This plan will be implemented in Q1 FY18 and will include training to relevant personnel about the new standardized process.

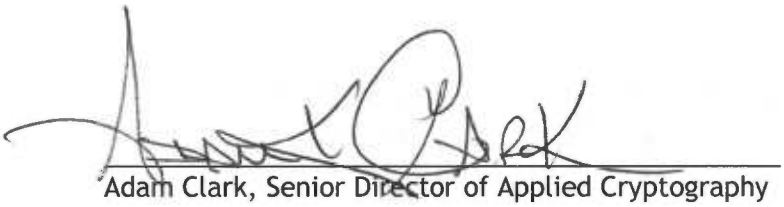
Visa
44901 RUSSELL BRANCH PARKWAY
ASHBURN, VA 201472913

	has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement; • The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); • The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; • The CA is made aware of a material change in the information contained in the Certificate; • The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; • The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; • The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; • The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; • The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; • Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or		

Visa
44901 RUSSELL BRANCH PARKWAY
ASHBURN, VA 201472913

	• The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time). (See SSL Baseline Requirements Section 13.1.5)		
2 - 4.1 2 - 4.2 2 - 4.3	The CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate. (SSL Baseline Requirements Section 11.1) The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements: • Identity (SSL Baseline Requirements Section 3.2.2.1) • DBA/Trade name (SSL Baseline Requirements Section 3.2.2.2) • Authenticity of Certificate Request (SSL Baseline Requirements Section 3.2.5) • Verification of Individual Applicant (SSL Baseline Requirements Section 3.2.3) • Verification of Country (SSL Baseline Requirements Section 3.2.2.3) The CA maintains controls and procedures to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification. (See SSL Baseline Requirements Section 11.2)	We were unable to obtain evidence of the domain validation documentation for a certificate issued.	Visa notes a plan to standardize and establish consistency across all Domain Validations to include our internal certificate requests, is in progress. This plan will be implemented in Q1 FY18 and include training to relevant personnel about the new standardized process.

Visa
44901 RUSSELL BRANCH PARKWAY
ASHBURN, VA 201472913



Adam Clark, Senior Director of Applied Cryptography

Visa
44901 RUSSELL BRANCH PARKWAY
ASHBURN, VA 201472913

APPENDIX A - IN-SCOPE CAs

Root CA's

CA Name	Serial Number	SHA1 Thumbprint
CN = Visa eCommerce Root OU = Visa International Service Association O = VISA C = US	13 86 35 4d 1d 3f 06 f2 c1 f9 65 05 d5 90 1c 62	70 17 9b 86 8c 00 a4 fa 60 91 52 22 3f 9f 3e 32 bd e0 05 62
CN = Visa eCommerce Root CA - G2 OU = Visa International Services Association O = VISA L = Ashburn S = Virginia C = US	51 3e 96 00 00 00 68 10 fc 6e 08 a3 d6 14 67	fc 7e fd 44 ef b6 9a e2 12 f3 47 41 68 5f 90 ec ca 6b 0d a8

Issuing CA

CA Name	Serial Number	SHA1 Thumbprint
CN = Visa eCommerce Issuing CA OU = Visa International Service Association O = VISA C = US	00 d8 74 61 30 41 fc 3c 44 a0 bc c6 5d 6c 36 f1 10	80 7a 77 b2 44 51 57 6c fb 3f b9 1e 97 73 52 27 fa b4 04 dd