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

101 S Hanley Rd, Suite 800
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined for Visa's certification authority ("CA") operations at Highlands Ranch, Colorado and Ashburn, Virginia for,

- Visa's disclosure of its SSL certificate lifecycle 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 its disclosed practices

- the effectiveness of its controls over:
  - key and SSL certificate integrity;
  - the authenticity and confidentiality of SSL subscriber and relying party information;
  - continuity of key and SSL certificate lifecycle management operations;
  - development, maintenance, and operation of CA systems integrity; and
  - meeting the network and certificate system security requirements set forth by the CA/Browser Forum

throughout the period April 1, 2017 to March 31, 2018, for its CAs enumerated in Attachment A in scope for SSL Baseline Requirements and Network Security Requirements.

Visa's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.2. Our responsibility is to express an opinion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period April 1, 2017 to March 31, 2018, for its CAs enumerated in Attachment A, in all material respects, Visa:

- disclosed its SSL certificate lifecycle management business practices, enumerated in Attachment B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Visa repository

- provided such services in accordance with its disclosed practices

- maintained effective controls over:
  - key and SSL certificate integrity;
  - the authenticity and confidentiality of SSL subscriber and relying party information;
  - continuity of key and SSL certificate lifecycle management operations;
  - development, maintenance, and operation of CA systems integrity; and
  - meeting 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 2.2.

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.

During our examination, we noted the following which caused a qualification of our opinion:

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		**Control Deficiency Noted**
2-2.5	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated after the Effective Date (1 July 2012) conform to the Baseline Requirements.	For 11 of the 45 certificate issuances selected, we noted the extended key usage field was not present in accordance with the Baseline Requirements.
2-5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The CA obtains evidence that the Certificate was misused;	For 7 of the 21 certificate revocation requests selected, the revocation was not completed within the twenty-four hour requirement.

	5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 6. The CA is made aware of any circumstance indicating that use of a FullyQualified 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); 7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 8. The CA is made aware of a material change in the information contained in the Certificate; 9. 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; 10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 12. 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; 13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; 14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 15. 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).	

2-5.10	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	The OCSP responder was configured to allow a response of "good" for a certificate that was not issued by the CA, until February 13, 2018.
2-7.3	The CA maintains controls to provide reasonable assurance that audit logs generated after the Effective Date (1 July 2012) are retained for at least seven years.	We were unable to obtain evidence that firewall and router activity logs were being retained for the required seven year period.

In our opinion, except for the effect of the matters described in the preceding table, throughout the period April 1, 2017 to March 31, 2018, Visa has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices, enumerated in Attachment B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Visa repository

- provided such services in accordance with its disclosed practices

- maintained effective controls over:
  - key and SSL certificate integrity;
  - the authenticity and confidentiality of SSL subscriber and relying party information;
  - continuity of key and SSL certificate lifecycle management operations;
  - development, maintenance, and operation of CA systems integrity; and
  - meeting 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 2.2.

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 2.2, nor the suitability of any of Visa's services for any customer's intended purpose.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
August 20, 2018

ATTACHMENT A - IN-SCOPE CAs

Root CAs

CA Name	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint

CN = Visa Information Delivery Root CA
OU = Visa International Service Association
O = VISA
C = US
	5b 57 d7 a8 4c b0 af d9 d3 6f 4b a0 31 b4 d6 e2	5a 4d 0e 8b 5f dc fd f6 4e 72 99 a3 6c 06 0d b2 22 ca 78 e4	c5 7a 3a cb e8 c0 6b a1 98 8a 83 48 5b f3 26 f2 44 87 75 37 98 49 de 01 ca 43 57 1a f3 57 e7 4b

CN = Visa Information Delivery Root CA - G2
OU = Visa International Services Association
O = VISA
L = Ashburn
S = Virginia
C = US
	51 3e 96 00 00 00 67 2a a4 73 c8 f7 e7 6e 93	61 f5 1e 6a 12 89 39 6a 82 d9 34 7d c9 73 05 57 a4 91 15 5f	0b f5 b2 a9 70 4a ab 1a 44 76 28 3f 61 0e a3 7a c7 f1 04 75 45 ba 0c 46 f7 27 07 82 8b 05 78 ee

Issuing CAs

CA Name	Serial Number	SHA1 Thumbprint	SHA 2 Thumbprint

CN = Visa Information Delivery Internal CA
OU = Visa International Service Association
O = VISA
C = US
	22 b0 8f eb ca 60 17 41 68 5f 05 f4 88 e0 f2 c2	b8 e5 c9 b4 42 b7 3f fe bd 21 8f 9a 18 94 8a 70 bd 3b a7 1f	e7 37 3a 39 c2 35 47 27 0e 3d 20 b2 47 87 5f a4 43 f4 f2 b6 65 d5 16 26 01 91 39 90 38 37 66 d3

CN = Visa Information Delivery External CA
OU = Visa International Service Association
O = VISA
C = US
	17 b4 6e 88 61 1d b7 9c f6 28 47 8e 22 89 85 ed	6f c9 20 c3 f4 3b 4d ba c7 15 7e d7 33 2b 7c 46 da a3 54 ce	b8 63 a8 f0 f8 de bc 79 b8 9d 87 de 94 1f 6f 15 ec 35 77 15 fa 0c f8 0e 84 b7 a6 cd bd 8d 34 43

ATTACHMENT B - POLICY VERSIONS IN-SCOPE

Certificate Policies

Policy Name	Version	Date
Visa Public Key Infrastructure Certificate Policy (CP)	3.3	March 29, 2018
Visa Public Key Infrastructure Certificate Policy (CP)	3.2	January 31, 2018
Visa Public Key Infrastructure Certificate Policy (CP)	3.1	March 31, 2017

Certification Practice Statements

Policy Name	Version	Date
Visa Public Key Infrastructure Certificate Practice Statement (CPS)	3.3	March 29, 2018
Visa Public Key Infrastructure Certificate Practice Statement (CPS)	3.2	January 31, 2018
Visa Public Key Infrastructure Certificate Practice Statement (CPS)	3.1	March 31, 2017

Monday, August 20, 2018

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 Information Delivery CAs, listed in Attachment A in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

Visa's 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, 2017 to March 31 2018, Visa has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - applicable versions of the Visa Public Key Infrastructure Certification Practice Statement ("CPS") and Visa Public Key Infrastructure Certificate Policy ("CP") enumerated in Attachment B;
  - 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 2.2, 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

2-2.5	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated after the Effective Date (1 July 2012) conform to the Baseline Requirements.	For 11 of the 45 certificate issuances selected, we noted the extended key usage field was not present in accordance with the Baseline Requirements.	Visa notes an incorrect template was used as it did not contain an extended key usage (EKU) field. Subsequently, this was corrected by adding the required EKU field. Management notes that the issue has been remediated.
2-5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The CA obtains evidence that the Certificate was misused; 5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 6. The CA is made aware of any circumstance indicating that use of a FullyQualified 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	For 7 of the 21 certificate revocation requests selected, the revocation was not completed within the twenty-four hour requirement.	Visa notes a plan to standardize and establish consistency across all Domain Validations & Revocations. Visa requested certificate revocations will be required to use a centralized system that will enforce specific requirements. This plan will be completed by Q4 fiscal year 2018 and includes training to relevant personnel about the new standardized process.

	agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 8. The CA is made aware of a material change in the information contained in the Certificate; 9. 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; 10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 12. 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; 13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; 14. Revocation is required by the CA's Certificate Policy		

	and/or Certification Practice Statement; or 15. 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).		
2-5.10	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	The OCSP responder was configured to allow a response of "good" for a certificate that was not issued by the CA, until February 13, 2018.	Visa notes the OCSP responder product deployed at the time was defective for which the vendor was unable to provide an acceptable resolution. As a result, Visa ceased operation of the faulty product and subsequently deployed an alternate solution. Management notes that the issue has been remediated.
2-7.3	The CA maintains controls to provide reasonable assurance that audit logs generated after the Effective Date (1 July 2012) are retained for at least seven years.	We were unable to obtain evidence that firewall and router activity logs were being retained for the required seven year period.	Visa notes the current firewall log retention requirements follow Visa's global retention policy which do not align with WTBR's requirements. As a result, Visa will work with the relevant teams to determine the appropriate actions needed to align with the seven-year requirement.

Adam Clark
Senior Director of Applied Cryptography
August 20, 2018

ATTACHMENT A - IN-SCOPE CAs

Root CAs

CA Name	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint

CN = Visa Information Delivery Root CA
OU = Visa International Service Association
O = VISA
C = US
	5b 57 d7 a8 4c b0 af d9 d3 6f 4b a0 31 b4 d6 e2	5a 4d 0e 8b 5f dc fd f6 4e 72 99 a3 6c 06 0d b2 22 ca 78 e4	c5 7a 3a cb e8 c0 6b a1 98 8a 83 48 5b f3 26 f2 44 87 75 37 98 49 de 01 ca 43 57 1a f3 57 e7 4b

CN = Visa Information Delivery Root CA - G2
OU = Visa International Services Association
O = VISA
L = Ashburn
S = Virginia
C = US
	51 3e 96 00 00 00 67 2a a4 73 c8 f7 e7 6e 93	61 f5 1e 6a 12 89 39 6a 82 d9 34 7d c9 73 05 57 a4 91 15 5f	0b f5 b2 a9 70 4a ab 1a 44 76 28 3f 61 0e a3 7a c7 f1 04 75 45 ba 0c 46 f7 27 07 82 8b 05 78 ee

Issuing CAs

CA Name	Serial Number	SHA1 Thumbprint	SHA 2 Thumbprint

CN = Visa Information Delivery Internal CA
OU = Visa International Service Association
O = VISA
C = US
	22 b0 8f eb ca 60 17 41 68 5f 05 f4 88 e0 f2 c2	b8 e5 c9 b4 42 b7 3f fe bd 21 8f 9a 18 94 8a 70 bd 3b a7 1f	e7 37 3a 39 c2 35 47 27 0e 3d 20 b2 47 87 5f a4 43 f4 f2 b6 65 d5 16 26 01 91 39 90 38 37 66 d3

CN = Visa Information Delivery External CA
OU = Visa International Service Association
O = VISA
C = US
	17 b4 6e 88 61 1d b7 9c f6 28 47 8e 22 89 85 ed	6f c9 20 c3 f4 3b 4d ba c7 15 7e d7 33 2b 7c 46 da a3 54 ce	b8 63 a8 f0 f8 de bc 79 b8 9d 87 de 94 1f 6f 15 ec 35 77 15 fa 0c f8 0e 84 b7 a6 cd bd 8d 34 43

ATTACHMENT B - POLICY VERSIONS IN-SCOPE

Certificate Policies

Policy Name	Version	Date
Visa Public Key Infrastructure Certificate Policy (CP)	3.3	March 29, 2018
Visa Public Key Infrastructure Certificate Policy (CP)	3.2	January 31, 2018
Visa Public Key Infrastructure Certificate Policy (CP)	3.1	March 31, 2017

Certification Practice Statements

Policy Name	Version	Date
Visa Public Key Infrastructure Certificate Practice Statement (CPS)	3.3	March 29, 2018
Visa Public Key Infrastructure Certificate Practice Statement (CPS)	3.2	January 31, 2018
Visa Public Key Infrastructure Certificate Practice Statement (CPS)	3.1	March 31, 2017