KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Visa, Inc. (“VISA”):

We have examined for its Certification Authority (CA) operations at Highlands Ranch, Colorado and Ashburn, Virginia, 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 website, 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 lifecycle 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 as of March 31, 2016 for its Information Delivery Root CA, Visa Information Delivery Root CA – G2, VICA1, VICA2, Visa Information Delivery Internal CA, Visa Information Delivery External CA, Visa Corporate Email Sub CA, and Visa Corporate Email Issuing CA (collectively referred to as the “Visa Information Delivery CAs”) and its eCommerce Root CA, Visa eCommerce Root CA – G2, eCommerce Issuing CA, eVisa Sub CA, CEMEA CA, and Canada CA (collectively referred to as the “Visa eCommerce CAs”).

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 v2.0, 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) evaluating the suitability of the design of the controls; and
(3) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

During our examination, we noted the following matters:

	Matters Noted	Impacted WebTrust Criteria
1	Four instances were noted where eCommerce SHA-1 certificates were issued after the January 1, 2016 deadline specified within the CA Browser Forum Baseline SSL requirements. Noted that the expiration date of these certificates was prior to December 31, 2016.	This caused WebTrust Criterion 2-2.1 (below) to not be met: 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: ● Validity Period (See SSL Baseline Requirements Section 9.4)
2	Visa did not obtain executed Subscriber or Terms of Use Agreements for all certificates signed by Information Delivery or eCommerce.	This caused WebTrust Criterion 2-3.1 (below) to not be met: The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant: 1. A certificate request, which may be electronic; and 2. An executed Subscriber or Terms of Use Agreement, which may be electronic. 3. Any additional documentation the CA determines necessary to meet the Baseline Requirements.
3	Visa has a detailed corporate onboarding process for new clients who may ultimately require publicly trusted SSL certificates to do business with VISA. However, it was noted that the VISA CA's vetting procedures do not specifically address the referenced WTBR criteria at the time of certificate issuance for the verification of the O, OU, L, C attributes. It was also noted that the VISA CA uses an internal system (VISA Profiler), to verify client organization and individual information, but there is no process in place to validate that information by using a third-party database considered a Reliable Data Source or attestation letters.	This caused WebTrust Criteria 2-2.3, 2-4.6, and 2-4.9 (below) to not be met: 2-2.3 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 SSL Baseline Requirements including the following: • The CA shall implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with SSL Baseline Requirements Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with SSL Baseline Requirements Section 11.2. 4-4.6 The CA maintains controls and procedures to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 11 of SSL Baseline Requirements to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to issuing the Certificate 4.9 The CA maintains controls and procedures to provide reasonable assurance that, prior to using a

	Matters Noted	Impacted WebTrust Criteria
		data source, the CA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in section 11.6 of the SSL Baseline Requirements. Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation: 1. The age of the information provided, 2. The frequency of updates to the information source, 3. The data provider and purpose of the data collection, 4. The public accessibility of the data availability, and 5. The relative difficulty in falsifying or altering the data. Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under Section 11.
4	Verification of the Fully-Qualified Domain Name(s) and IP address(es) listed in the certificates is not formally performed and documented per Baseline Requirements.	This caused WebTrust Criterion 2-4.1 (below) to not be met: 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.
5	Visa's CPS specified the requirement for a quarterly self-assessment for three percent (3%) of the Certificates issued. However, a process for performing such quarterly assessments was not fully designed and implemented as of 3/31/16.	This caused WebTrust Criterion 2-8.2 (below) to not be met: The CA maintains controls to provide reasonable assurance that: • it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken,

	Matters Noted	Impacted WebTrust Criteria
6	Visa has an annual risk assessment process that evaluates a broad set of corporate security risks and the encryption methods and practices in place. However, it was noted that the risk assessment did not specifically address the following: - the potential internal and external threats of any Certificate Data or Certificate Management Processes - the likelihood of these threats, considering the sensitivity of the Certificate Data and Certificate Management Processes - the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.	This caused WebTrust Criterion 3.2 (below) to not be met: 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.
7	Evidence was not available to demonstrate the completion of user account reviews for all CA and RA systems at least every 90 days to deactivate accounts no longer necessary for operations.	This caused WebTrust Criterion 4-2 (below) to not be met: The CA maintains controls to provide reasonable assurance that: • Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;

In our opinion, except for the matters described in the preceding paragraphs, as of March 31, 2016, VISA has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices in its:
  - VISA Public Key Infrastructure Certification Policy (CP), dated March 3, 2016 on the VISA website; and
  - VISA Public Key Infrastructure Certification Practice Statement (CPS), dated March 3, 2016

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

- suitably designed, and placed into operation, 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 (for the registration activities performed by VISA)

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, 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 v2.0.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of VISA's controls, individually or in the aggregate.

The suitability of the design of the 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 suitability of the design of the 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.

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 v2.0, nor the suitability of any of VISA's services for any customer's intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, California
September 16, 2016

Assertion of Management as to
Its Disclosure of its Business Practices and its Controls
Over its Certification Authority Operations
as of March 31, 2016

September 16, 2016

VISA, Inc. ("VISA") provides its SSL certification authority (CA) services through the Information Delivery Root CA, Visa Information Delivery Root CA – G2, VICA1, VICA2, Visa Information Delivery Internal CA, Visa Information Delivery External CA, Visa Corporate Email Issuing CA (VCEICA), and Visa Corporate Email Sub CA (collectively referred to as the “Visa Information Delivery CAs”) and its eCommerce Root CA, Visa eCommerce Root CA – G2, eCommerce Issuing CA, eVisa Sub CA, CEMEA CA, and Canada CA (collectively referred to as the “Visa eCommerce CAs”).

The management of VISA is responsible for suitably designing and implementing controls over its CA operations, including 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 website, 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 lifecycle 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. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even suitably designed and implemented controls can only provide reasonable assurance with respect to VISA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of VISA has assessed the disclosure of its certificate practices and the design of its controls over its Visa Information Delivery CAs and Visa eCommerce CAs. Based on that assessment, in VISA’s Management’s opinion, in providing its CA services at Highlands Ranch, Colorado and Ashburn, Virginia, as of March 31, 2016:

- VISA disclosed its SSL certificate lifecycle management business practices in its:
    - VISA Public Key Infrastructure Certification Policy (CP), dated March 3, 2016 on the VISA website; and
    - VISA Public Key Infrastructure Certification Practice Statement (CPS), dated March 3, 2016 (restricted to authorized users and provided by Visa upon request)

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

- VISA suitably designed, and placed into operation, 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 (for the registration activities performed by VISA)

- VISA suitably designed, and placed into operation, 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

- VISA suitably designed, and placed into operation, 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 v2.0 except for the effects of the matters noted below:

	Matters Noted	**Impacted WebTrust Criteria**
1	Four instances were noted where eCommerce SHA-1 certificates were issued after the January 1, 2016 deadline specified within the CA Browser Forum Baseline SSL requirements. Noted that the expiration date of these certificates was prior to December 31, 2016. *In July 2014, Visa established a worldwide PKI roadmap to end enterprise-wide SHA-1 trust in 1/1/2017. The roadmap schedule considered our client constraints, as well as alignment with industry/CABF standards to end SHA-1 trust by 1/1/2017. As of April 8, 2016 SHA-1 certificates are no longer issued. Management notes that the issue has been remediated.*	This caused WebTrust Criterion 2-2.1 (below) to not be met: 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: • Validity Period (See SSL Baseline Requirements Section 9.4)
2	Visa did not obtain executed Subscriber or Terms of Use Agreements for all certificates signed by Information Delivery or eCommerce. *Visa notes that a Subscriber agreement has been integrated into all electronic certificate requests for Information Delivery and eCommerce certificates and must be accepted before the requests can be submitted. Management notes that the issue has been remediated.*	This caused WebTrust Criterion 2-3.1 (below) to not be met: The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant: 1. A certificate request, which may be electronic; and 2. An executed Subscriber or Terms of Use Agreement, which may be electronic. 3. Any additional documentation the CA determines necessary to meet the Baseline Requirements.

	Matters Noted	Impacted WebTrust Criteria
3	Visa has a detailed corporate onboarding process for new clients who may ultimately require publicly trusted SSL certificates to do business with VISA. However, it was noted that the VISA CA's vetting procedures do not specifically address the referenced WTBR criteria at the time of certificate issuance for verification of the O, OU, L, C attributes. It was also noted that the VISA CA uses an internal system (VISA Profiler) to verify client organization and individual information, but there is no process in place to validate that information by using a third-party database considered a Reliable Data Source or attestation letters. *Management has a plan to document and implement an enhanced vetting procedure in Q1 FY17 that leverages existing client onboarding processes to verify the O, OU, L, C attributes in accordance with the Baseline Requirements.*	This caused WebTrust Criteria 2-2.3, 2-4.6, and 2-4.9 (below) to not be met: 2-2.3 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 SSL Baseline Requirements including the following: • The CA shall implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with SSL Baseline Requirements Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with SSL Baseline Requirements Section 11.2. 4-4.6 The CA maintains controls and procedures to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 11 of SSL Baseline Requirements to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to issuing the Certificate 4.9 The CA maintains controls and procedures to provide reasonable assurance that, prior to using a data source, the CA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in section 11.6 of the SSL Baseline Requirements. Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation: 1. The age of the information provided, 2. The frequency of updates to the information source, 3. The data provider and purpose of the data collection, 4. The public accessibility of the data availability, and 5. The relative difficulty in falsifying or altering the data. Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under Section 11.

	Matters Noted	**Impacted WebTrust Criteria**
4	Verification of the Fully-Qualified Domain Name(s) and IP address(es) listed in the certificates is not formally performed and documented per Baseline Requirements. *Visa notes that a formal process was subsequently implemented whereby Fully-Qualified Domain Name(s) and IP address(es) listed in the certificate are vetted according to the CP, CPS and the Baseline Requirements. If there is a discrepancy with the whois information for the domain, a domain attestation is sent to the domain owner for approval. Management notes that the issue has been remediated.*	This caused WebTrust Criterion 2-4.1 (below) to not be met: 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.
5	Visa's CPS specified the requirement for a quarterly self-assessment for three percent (3%) of the Certificates issued. However, a process for performing such quarterly assessments was not fully designed and implemented as of 3/31/16. *Visa notes the 3% self-audit was approved and documented in our CPS prior to the start of the point in time audit (3/31/16). The quarterly 3% self-audits were subsequently commenced and the initial quarterly results were published on 6/30/2016. The self-audits were completed as prescribed by our CP, CPS and the Baseline Requirements. Management notes that the issue has been remediated.*	This caused WebTrust Criterion 2-8.2 (below) to not be met: The CA maintains controls to provide reasonable assurance that: • it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken,

	Matters Noted	**Impacted WebTrust Criteria**
6	Visa has an annual risk assessment process that evaluates a broad set of corporate security risks and the encryption methods and practices in place. However, it was noted that the risk assessment did not specifically address the following: - the potential internal and external threats of any Certificate Data or Certificate Management Processes - the likelihood of these threats, considering the sensitivity of the Certificate Data and Certificate Management Processes - the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. *Visa notes that, in addition to the global risk assessment and a separate Business Impact Analysis on the PKI Infrastructure, a targeted risk assessment that leverages the results of other ongoing risk assessments will be performed to meet Baseline Requirements. Visa has a plan to conduct the targeted PKI risk assessment in Q1 FY2017.*	This caused WebTrust Criterion 3.2 (below) to not be met: 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.
7	Evidence was not available to demonstrate the completion of user account reviews for all CA and RA systems at least every 90 days to deactivate accounts no longer necessary for operations. *Visa has implemented an enhanced user access review process for CA and RA systems, with formal documentation to meet Baseline Requirements. Management notes that the issue has been remediated.*	This caused WebTrust Criterion 4-2 (below) to not be met: The CA maintains controls to provide reasonable assurance that: • Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;

Visa, Inc.

Shirish Puranik
Vice President – Access and Payment Security