To Whom It May Concern:

Your request for a copy of the CyberSource SSAE-16 Report has been referred to me.

Enclosed is the report from our independent auditors, KPMG, which contains an opinion letter evidencing CyberSource's compliance with a comprehensive internal controls structure. The report also contains the detailed control procedures and testing performed by KPMG. The purpose of this report is to assist internal and external auditors of client organizations in evaluating the controls in place over client processing performed by CyberSource.

Please feel free to contact me at dchan@visa.com if you need any further information.

Sincerely,

David Chan
Sr. Business Leader
Global Compliance

Visa Inc.
P.O. Box 8999
San Francisco, CA 94128-8999
U.S.A.

CyberSource®

January 5, 2016

Andre Machicao
Senior Vice President
CyberSource Corporation
900 Metro Center Blvd.
Foster City, CA 94404

Dear Client:

As of September 30, 2015, a SSAE16 attestation (fka SAS 70) was completed by KPMG on the electronic payment and risk management activities of CyberSource Corporation ("CyberSource") and Authorize.Net, a solution of CyberSource. That report is available to clients upon request.

In the report, the auditors have stated that in their opinion the accompanying description of controls presents fairly, in all material respects, the relevant aspects of CyberSource controls that have been placed in operation throughout the period of October 1, 2014 to September 30, 2015. Also, in their opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the CyberSource controls. Finally, in their opinion, the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period.

Management relies on a risk assessment framework, which provides an on-going review of the effectiveness of CyberSource's system of internal controls. Since the release of the SSAE16 report covering the period from October 1, 2014 to September 30, 2015, there have been no significant observations that have been brought to the attention of management concerning the internal control objectives supporting electronic payment and risk management services. Management believes that the internal control objectives supporting electronic payment and risk management services continue to be achieved.

Sincerely,

Andre Machicao
Senior Vice President, CyberSource and Authorize.Net

CyberSource

Report on Controls Placed in Operation and Tests of Operating Effectiveness for CyberSource Electronic Payment, Fraud Management and Payment Security Services and Authorize.Net Electronic Payment and Fraud Risk Management Services

October 1, 2014 through September 30, 2015

KPMG LLP
55 Second Street
San Francisco, CA 94105

Independent Service Auditors' Report

Board of Directors of CyberSource Corporation
Foster City, CA

Scope of Report

We have examined CyberSource Corporation's ("CyberSource") description of its system for their controls related to (i) General controls and transactional controls for CyberSource's Electronic Payment, Fraud Management, and Payment Security Services and (ii) General controls and transactional controls for Electronic Payment Services and Fraud Risk Management Services provided by Authorize.Net, a solution of CyberSource, (collectively referred to as the "Electronic Payment, Fraud Management and Payment Security Services system") throughout the period October 1, 2014 to September 30, 2015 (description) and the suitability of design and the operating effectiveness of controls to achieve the related control objectives stated in the description.

The description indicates that certain control objectives specified in the description can be achieved only if complementary client organization controls contemplated in the design of CyberSource's controls are suitably designed and operating effectively, along with related controls at the subservice organizations. We have not evaluated the suitability of the design or operating effectiveness of such complementary client organization controls.

CyberSource uses the following subservice organizations:

Subservice Organizations	Location	Service Role
XO Communications Internap	Colorado	Recovery data center co-location, environmental control systems, and Internet connectivity from October 1, 2014 to January 25, 2015. Production systems housed in Visa Facility from Jan 26, 2015 through September 30, 2015.
Internap Savvis	England	Peering point and protocol conversion

The description in Section 3 and Section 4 includes only the controls and related control objectives of CyberSource and excludes the control objectives and related controls of the above subservice organizations. Our examination did not extend to controls of the above subservice organizations.

The information in Section 5 of management's description of the service organization's Electronic Payment, Fraud Management and Payment Security Services system, "Other Information Provided by CyberSource," that describes Security Certification and Validation, Legal Compliance, Privacy Policy, and Disaster Recovery/Business Continuity, is presented by management of CyberSource to provide additional information and is not a part of CyberSource's description of its Electronic Payment, Fraud Management and Payment Security Services system made available to client organizations during the period October 1, 2014 to September 30, 2015. Information about Security Certification and Validation, Legal Compliance, Privacy Policy, and Disaster Recovery/Business Continuity has not been subjected to the procedures applied in the examination of the description of the Electronic Payment, Fraud Management and Payment Security Services system and of the suitability of the design and operating

effectiveness of controls to achieve the related control objectives stated in the description of the Electronic Payment, Fraud Management and Payment Security Services system, and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

In its description in Section 2, CyberSource has provided an assertion about the fairness of the presentation of the description and the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description. CyberSource is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting and using suitable criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, the controls were suitably designed, and the controls were operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2014 to September 30, 2015.

An examination of a description of a service organization's Electronic Payment, Fraud Management and Payment Security Services system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and the operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in CyberSource's assertion:

(a) the description fairly presents the Electronic Payment, Fraud Management and Payment Security Services system that was designed and implemented throughout the period October 1, 2014 to September 30, 2015,

(b) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2014 to September 30, 2015, and

(c) the controls tested, which together with the complementary client organization controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description in Section 4 were achieved and operated effectively throughout the period October 1, 2014 to September 30, 2015.

Description of Tests of Controls

The specific controls and the nature, timing, extent, and results of the tests are listed in Section 4.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of CyberSource, its affiliates, client organizations of CyberSource's Electronic Payment, Fraud Management and Payment Security Services system during some or all of the period October 1, 2014 to September 30, 2015, and the independent auditors of such client organizations, who have a sufficient understanding to consider it, along with other information including information about controls implemented by client organizations themselves, when assessing the risks of material misstatements of client organizations' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

October 23, 2015
San Francisco, CA

CyberSource

We have prepared CyberSource Corporation's ("CyberSource") description of our system applicable to (i) General controls and transactional controls for CyberSource's Electronic Payment, Fraud Management, and Payment Security Services and (ii) General controls and transactional controls for Electronic Payment Services and Fraud Risk Management Services provided by Authorize.Net, a solution of CyberSource, (collectively referred to as the "Electronic Payment, Fraud Management and Payment Security Services system") for client organizations of the Electronic Payment, Fraud Management and Payment Security Services system during some or all of the period of October 1, 2014 to September 30, 2015, and the client organizations' independent auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by client organizations of the Electronic Payment, Fraud Management and Payment Security Services system themselves, when assessing the risks of material misstatements of client organizations' financial statements. We confirm, to the best of our knowledge and belief that:

1) The accompanying description in Section 3 and Section 4, fairly presents our Electronic Payment, Fraud Management and Payment Security Services system applicable to (i) Electronic Payment, Fraud Management, and Payment Security Services and (ii) Electronic Payment Services and Fraud Risk Management Services provided by Authorize.Net made available to client organizations of the Electronic Payment, Fraud Management and Payment Security Services system during some or all of the period of October 1, 2014 to September 30, 2015.

   CyberSource uses the following subservice organizations:

Subservice Organizations	Location	Service Role
XO Communications Internap	Colorado	Recovery data center co-location, environmental control systems, and Internet connectivity from October 1, 2014 to January 25, 2015. Production systems housed in Visa Facility from Jan 26,2015 to September 30, 2015.
Internap Savvis	England	Peering point and protocol conversion

   The description in Section 3 and Section 4 includes only the controls and related control objectives of CyberSource and excludes the control objectives and related controls of the aforementioned subservice organizations.

   The criteria we used in making this assertion were that the accompanying description:

   a) Presents how the Electronic Payment, Fraud Management and Payment Security Services system made available to client organizations of the system was designed and implemented to process relevant transactions, including:

      - The types of services provided, including, as appropriate, the classes of transactions processed;
      - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for client organizations;
      - The related accounting records, supporting information and specific accounts that were used to initiate, authorize, record, process and report transactions; this includes the correction of

CyberSource

incorrect information and how information was transferred to the reports prepared for client organizations;
- How the Electronic Payment, Fraud Management and Payment Security Services system captured and addressed significant events and conditions, other than transactions;
- The process used to prepare reports or other information for client organizations;
- Specified control objectives and controls designed to achieve those objectives;
- Controls that we assumed, in the design of the Electronic Payment, Fraud Management and Payment Security Services system, would be implemented by client organizations, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us; and
- Other aspects of our control environment, risk assessment process, information systems and communication (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting client organizations' transactions.

b) Does not omit or distort information relevant to the scope of the Electronic Payment, Fraud Management and Payment Security Services system, while acknowledging that the description is prepared to meet the common needs of a broad range of client organizations and their independent auditors and may not, therefore, include every aspect of CyberSource's Electronic Payment, Fraud Management and Payment Security Services system that each individual client organization may consider important in its own particular environment.

2) The description includes relevant details of changes to CyberSource's Electronic Payment, Fraud Management and Payment Security Services system during the period covered by the descriptions.

3) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period of October 1, 2014 to September 30, 2015 to achieve those control objectives and subservice organizations applied the controls contemplated in the design of CyberSource controls. The criteria used in making this assertion were that:

a) The risks that threatened achievement of the control objectives stated in the description were identified;
b) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

October 23, 2015

Andre Machicao
Senior Vice President, Cybersource and Authorize.Net

Purpose

This report has been prepared to assist CyberSource (including Authorize.Net), client organizations of CyberSource during some or all of the period October 1, 2014 to September 30, 2015, and the independent auditors of such client organizations, when assessing the risks of material statements of client organizations' financial statements.

Report and Control Environment Changes

As part of ongoing operations, CyberSource makes changes to its operations and various support groups' roles and responsibilities to better align the business to service their client organizations. This report reflects changes that have occurred during the period.

Document Organization

KPMG conducted an examination in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements Section 801 "Reporting on Controls at a Service Organization" and International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board, of the following:

- CyberSource electronic payment, fraud management and payment security services
- Authorize.Net electronic payment and fraud risk management services

The report contains the following sections:

- Independent Service Auditors' Report Provided by KPMG
- Management's Assertion
- Introduction, Description of Operations, and Complementary Client Organization Controls
- Control Objectives, Related Controls, and Tests of Operating Effectiveness
- Other Information Provided by CyberSource

Overview of Operations

Company Background

CyberSource Corporation was founded in 1994 and was acquired by Visa Inc. on July 21, 2010. CyberSource provides electronic payment and risk management solutions. CyberSource Corporation is headquartered in Foster City, California. CyberSource acquired Authorize.Net on November 1, 2007. Authorize.Net is CyberSource's small online business. More than 450,000 businesses use CyberSource and Authorize.Net solutions, including half the companies comprising the Dow Jones Industrial Average. CyberSource regional operational locations are in Foster City, California; Miami, Florida; American Fork, Utah; Tokyo, Japan; the United Kingdom; Singapore and Sao Paulo, Brazil.

Product Overview

CyberSource offers a global payment management platform, providing secure electronic payment, fraud management, payment security and professional services to merchants and merchant service providers. CyberSource solutions help merchants transact across multiple sales channels worldwide, and are delivered as a cloud-based service, accessed through a single Internet connection. Solutions are packaged for merchant service providers, and merchants ranging in size from very small businesses to large multi-national corporations.

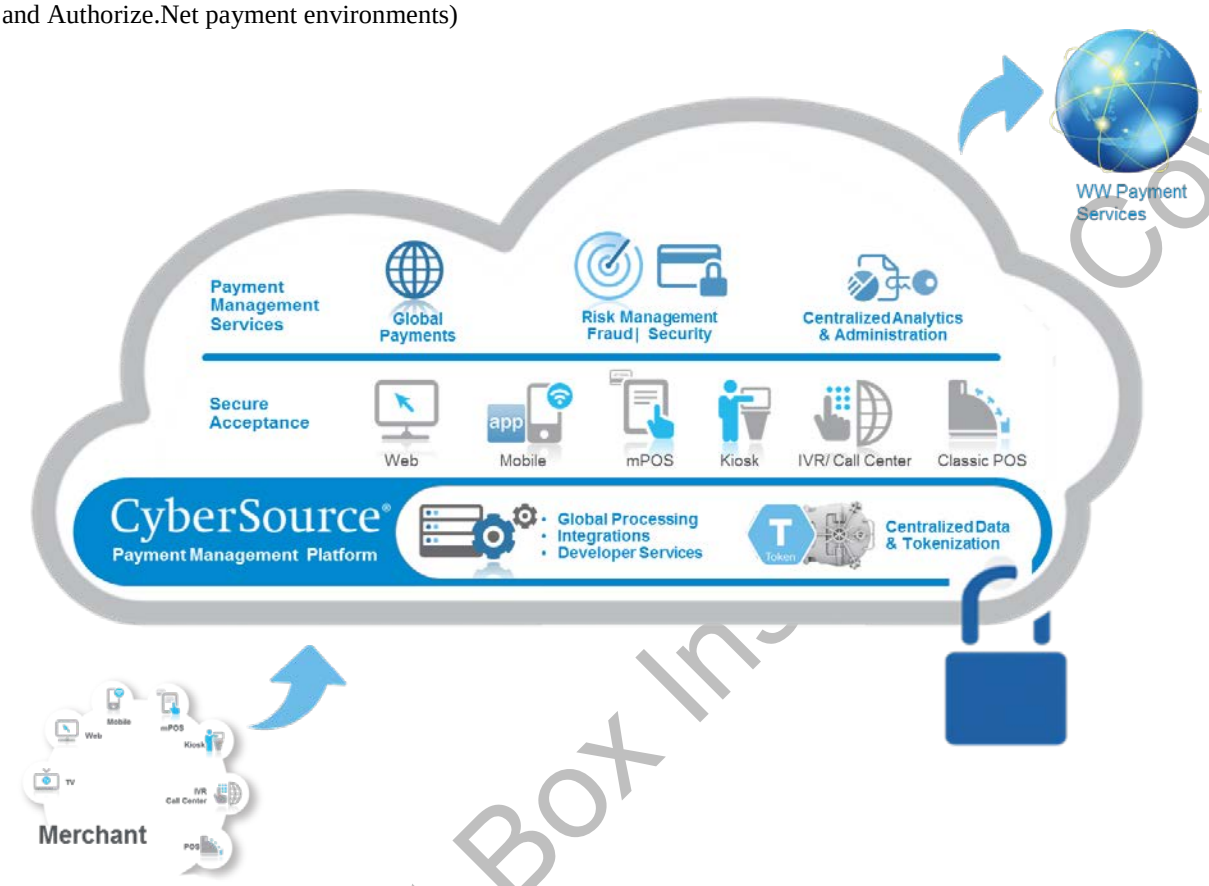
Payment & Payment Security Services — CyberSource provides brand-agnostic payment gateway services, enabling merchants to accept a wide range of payments across multiple sales channels (Web, mobile, mPOS, POS, IVR, call center, kiosk) worldwide, through a single Internet connection. CyberSource Secure Acceptance and payment tokenization services allow merchants to securely accept payments across multiple channels without payment data contacting merchant systems or being handled by call center staff. Global tax calculation and billing management services are also available via this same connection.

Fraud Management Services — Enterprise fraud management (EFM) solutions are delivered via the CyberSource Decision Manager system, accompanied by a suite of managed services offerings ranging from consulting and monitoring, to complete outsourcing of fraud operations. Fraud management tools for smaller businesses are made available through CyberSource's small business solution, Authorize.Net.

Analytics — The CyberSource platform provides an array of reporting and analytics services which consolidate payment activity across sales channels, processors and geographies, enabling merchants to better manage customer activity across channels, and gain insights to improve sales performance and operating efficiency.

Merchant Services Provider Solutions — CyberSource provides tools and services that enable acquiring banks, payment services providers and other partners to co-brand, resell and refer CyberSource and Authorize.Net brand solutions. The CyberSource through VisaNet connection method enables acquiring banks and processors to quickly adopt CyberSource services using their existing VisaNet connection.

Figure 1: CyberSource product overview for Payment Management Platform (applicable to both CyberSource and Authorize.Net payment environments)



Customers

CyberSource's customers range in size from small sole proprietorships to some of the world's largest corporations and institutions. To properly serve these diverse needs, CyberSource provides two separate solutions targeting different market segments as detailed below.

- CyberSource Enterprise Solution: Businesses that have high sales volume generally require the greatest range of payment options and the most sophisticated risk and management tools. These customers often sell in multiple countries and require support for local currencies and local payment options. High volume customers also frequently need to integrate payment processing with one or more internal business systems. Such high volume customers are serviced on CyberSource's enterprise platform including major airlines, online retailers, social media portals, and major telecom billers.

- CyberSource's Authorize.Net Solution: Smaller merchants generally seek simplicity and ease of use. CyberSource addresses these needs with the Authorize.Net platform, which offers numerous value-adding solutions including recurring billing and records tokenization.

Partners and Alliances

The CyberSource indirect sales channel has developed relationships with companies ranging from referral relationships to reselling CyberSource Enterprise services. Resellers include CyberSource services as part of their larger offering portfolio, facilitating the sale of our services. CyberSource resellers include financial institutions, ecommerce platform providers, application service providers, and specialized systems integrators. Referral partners are companies that refer merchants to CyberSource and CyberSource provides services directly to the referred merchants. Referral partners include companies from the payment industry, financial institutions, independent software vendors, integrators and consulting firms.

Authorize.Net targets prospective customers worldwide through a direct sales force as well as reseller and referral programs. Authorize.Net's ecosystem of over 7000 resellers and partners include small business resellers, payment service providers, some of the world's largest banks and processors and thousands of Independent Sales organizations (ISOs) and developers.

CyberSource Executive Management

The executive team of CyberSource is described below.

Andre Machicao is Senior Vice President of CyberSource within the Merchant Sales and Solutions group at Visa Inc. He is responsible for the Authorize.Net business and the Strategy, Product Management and Marketing functions for CyberSource. Mr. Machicao joined Visa in 2006. He previously held leadership positions within Visa's Strategy & Corporate Development and Global Product organizations where he focused on strategic initiatives related to new business opportunities and innovation in payments, including acquisitions, joint ventures, and venture investments for Visa. Prior to joining Visa, Mr. Machicao was a strategy and management consultant with Booz & Company. Before joining Booz, he held senior management positions within new business ventures, including CEO of industry2industry, a B2B eCommerce company. Previously, Mr. Machicao was an executive with Accenture's Center for Strategic Technology. Mr. Machicao holds a Bachelor of Science in Engineering from the University of California, Los Angeles and a Master of Business Administration from the University of California, Berkeley.

Paul Williamson is Vice President of Sales for CyberSource in North America within the Global Merchant Sales and Solutions group at Visa Inc. Mr. Williamson is responsible for Sales, Account

Management, Sales Engineering as well as our Channel business that includes our financial institution, technology, system integrator and reseller partners. Mr. Williamson joined Visa in 2013 and was initially Head of Revenue for PlaySpan where he focused on Sales, Strategy, and Go-to-Market planning. Prior to Visa Inc., Mr. Williamson was Vice President of Sales for Salesforce.com in their Mid-Market Business as well as holding a role in Strategic Sales. Before joining Salesforce.com, he held various senior management positions within the mobile, wireless POS and payments for the restaurant and hospitality industry at leading innovator, PalmTEQ Limited. Previously, Mr. Williamson was a consultant for a boutique research firm CyberResearch. He holds a Bachelor of Business in Marketing from Murdoch University, Perth Western Australia.

Francisco Rocha Campos ("Xiko"), is Head of Merchant Sales and Solutions, LAC, and is responsible for the CyberSource business included in that operating remit. Mr. Campos brings more than 25 years of experience to this role, and has worked in senior leadership roles in the financial services, travel and entertainment and IT industries in multiple locations across Latin and North America, Europe and Southeast Asia. Prior to joining Visa, Mr. Campos was a founding partner for an advisory company serving the needs of independent shareholders and investors and CEO of CVC, the largest tour and leisure travel distributor in Latin America. He previously worked at American Express where his roles included regional head for commercial cards in Latin America, head of consumer and small business products for Canada and general manager for commercial cards in Brazil.

J. Michael Bradley leads the CyberSource business in Asia Pacific, within the Merchant Sales and Solutions APAC organization, responsible for sales, business development, professional services, support, product management, and marketing. Mr. Bradley led the expansion of CyberSource from a Singapore representative office to in-market operations located in China, Hong Kong, Thailand, Korea, Singapore, Australia, and India. Prior to CyberSource, he was founder and president of Prelytic Software, Director of Risk Services at Visa International, Managing Director and Partner at Tribe LLC, and Founder of CentreBack Payments. He holds a Political Science degree from the University of San Diego and an MBA in International Business from the University of San Francisco.

Simon Stokes joined CyberSource in 2006 as UK head of sales, and was promoted to UK Managing Director in 2007, tasked with reaching out to the organization's existing customer base and building links with new prospects and partners. Attracted by the infancy and excitement of the eCommerce industry, Mr. Stokes witnessed 50% year-on-year company growth, and led an assessment of the addressable markets in Europe and Asia. In 2013, he was tasked with developing CyberSource Sales and Business operations in EMEA and APAC, creating an international team that latterly included Latin America and CyberSource Global Services. He is now responsible for CyberSource Global client and market development. Prior to joining CyberSource, Simon spent seventeen highly successful years with Dell in Europe, during which time the organization grew from just 20 to more than 1500 employees. At Dell, he gained experience in running sales and marketing teams, as well as managing accounts at a national and global level across the media, telecoms, banking, retail and manufacturing sectors.

Issa Keshek is Regional Director Central Europe/Middle East/Africa for CyberSource, responsible for defining and executing strategy for CyberSource across Central Europe/Middle East/Africa and leading business development and sales operations. Prior to joining CyberSource, Mr. Keshek was Regional Director Asia/Middle East/Africa for Clear2Pay N.V. Mr. Keshek's past experience includes managerial and sales leadership positions at Microsoft, CR2 and NCR. He holds a Bachelor of Science (B.Sc.), Computer Science, from the University of Jordan.

Internal Controls Integrated Framework

Risk Assessment

CyberSource employs a comprehensive risk management strategy consisting of three key components:

- **Identification & Assessment:** Determining potential risks against key controls, their likelihood of occurrence, and the resulting business impact of such an occurrence. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.
- **Risk Mitigation:** Prioritizing, evaluating, and implementing the appropriate risk reduction controls recommended during the risk assessment process. Risk mitigation controls cover a broad spectrum, including policies, procedures and baselines, technical controls, and insurance coverage.
- **Evaluation & Reassessment:** Continuous monitoring and assessment of the business environment as well as the evolving threat landscape to ensure that known and emerging risks are identified, assessed and reduced to a level deemed acceptable to the business.

Control Environment

The control environment represents the collective effect of specific controls. CyberSource's procedures include the following elements in this control environment:

- Organization and management.
- Personnel policies and procedures.
- Physical access controls.
- Management's control methods for monitoring and following up on performance, including information systems planning, and Information Systems (IS) policies and procedures.

Control Activities

CyberSource has adopted internationally recognized operations controls and security practices for secure data processing. Visa's (includes CyberSource) Key Controls, Policies, and Procedures ("Key Controls") were derived from the British Standard 7799, which has since been superseded by the International Standard ISO/IEC 17799. CyberSource policy and technical committees regularly review new ISO/IEC 17799 and ISO 27001 standards for applicability and adoption into the Key Controls.

The Operational Risk Sub-Committee (ORS) provides executive oversight for the Key Controls Information Security Policy. The ORS, or its subordinate working group, the Business Controls Working Group (BCWG), has the authority to approve exceptions to the Key Controls. The Business Controls Working Group Exceptions Approval Protocol determines the Sub-Committee or Working Group with approval authority for each exception based on risk. The BCWG meets monthly, or more often as needed, to review and approve exceptions submitted to Information Security.

Information and Communication

Communication processes include orientation and training programs for newly hired employees, continuing training programs, periodic meetings summarizing significant events and changes, use of electronic mail (email) to communicate time-sensitive messages and information, and the InSite "Intranet Portal" maintained by Visa. Security controls are documented on InSite, as maintained by Visa, and in the Employee Handbook, which contains information and procedures pertaining to issues such as security policies and physical security.

Monitoring

CyberSource monitors and analyzes the behavior of all critical application, network and server components using a combination of third party and internally developed monitoring tools. These tools enable CyberSource to perform fault monitoring and trend analysis for availability assurance, capacity planning and decision making purposes. In addition, security monitoring is performed utilizing the above as well as additional sensors including net flow, intrusion detection system (IDS) and deep packet inspection.

For subservice data center facilities (XO Communications), management periodically reviews the physical security and environmental controls and processes at those locations and follows up on findings. This is an identified control which is tested within Control Objective 2 - Physical Access of this report. During 2015, CyberSource applications were migrated from the subservicer's data center to Visa data centers (see Physical and Environmental Controls section below). As a result, the monitoring of these network and related systems is performed from within the Visa data centers.

The subservice organization, Internap Savvis, is a facility location which houses only network routers in secured cages and racks. These routers are a peering point and provides protocol conversion for CyberSource's internet traffic. The Visa Service Operations team monitors this traffic and network bandwidth in real-time to identify any technical issues needing troubleshooting.

Internal Audit

The Internal Audit function is established by the Audit and Risk Committee of Visa Inc.'s Board of Directors. The Internal Audit function provides independent assurance on the state of Visa's control, governance and compliance systems, and on emerging risks, including Visa's information systems environment. Internal Audit does this by evaluating the effectiveness of risk management, internal control, and governance processes.

Key aspects of the Internal Audit function and how it performs its assurance and advisory work are described below:

- Internal Audit is led by the Chief Auditor, who reports to directly to the Audit and Risk Committee and administratively to the Vice Chairman, Risk and Public Policy.
- Internal Audit performs an annual risk assessment to develop an annual internal audit plan which is reviewed and approved by the Audit and Risk Committee.
- Internal Audit provides appropriate reporting to the Audit and Risk Committee regarding the status of the audit plan, changes to the audit plan, significant observations, and related management action plans.
- Internal Audit is resourced with a professional internal audit staff with sufficient knowledge, skills, experience and professional certifications required to perform their work effectively, and is supplemented as needed by a third-party co-sourcing professional services firm. The staff includes information technology audit professionals who specialize in and perform internal audits of information systems and general computer controls.
- Internal Audit governs itself by adherence to The Institute of Internal Auditors mandatory guidance, including the *Code of Ethics* and the *International Standards for the Professional Practice of Internal Auditing*. This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit activity's performance.
- Audit Issues reported in internal audits are tracked and reported to Executive Management on a monthly basis, including any management plans extended beyond the original due date. Issues cannot be closed without the review and approval of Internal Audit. The status of open Audit Issues is periodically reported to Visa Inc.'s Audit and Risk Committee

Organizational Management

Goals and performance evaluations exist for IS (Information Systems) positions. Additionally, segregation of duties within the IS functions are as follows:

- Visa's Management and personnel are required to be independent of client institutions.
- Critical IS functions are organized into functional areas to provide for an appropriate segregation of duties, including:
  - Facilities and physical security
  - Information security
  - Processing operations
  - Network engineering and support
  - Enterprise systems engineering
  - Transaction services
  - Information services
  - Access and delivery solutions

Description of Control Activities

Personnel Policies

CyberSource conducts pre-screening background investigations in accordance with Visa Inc. policies. Prior to commencement of employment, background investigations are conducted to verify information provided by the applicant in the employment application and resume. Using a third party agency, CyberSource also conducts criminal background checks to identify convictions at the state and federal levels within the immediately preceding seven years.

Upon commencement of employment, each employee is required to review the employee handbook and to sign an acknowledgment form confirming that he/she has reviewed the handbook and understands the policies contained therein. Each employee is also required to sign an agreement regarding confidentiality and assignment of inventions. New hire orientation is mandatory for all new hires, during which time, the employee is further advised about company policies, security, and other terms relevant to his/her employment. Training of personnel is accomplished through supervised on-the-job training, classes, and seminars. Companywide performance reviews are conducted annually. More frequent reviews may be conducted on an individual basis as deemed necessary.

Physical and Environmental Controls

CyberSource's and Authorize.Net's production environments providing transaction services are hosted in Visa data centers located in Ashburn, VA – Operations Center East (OCE) and Highlands Ranch, CO – Operations Center Central (OCC).

Access to the CyberSource and Authorize.Net environments are limited to select individuals with operational responsibilities in the production environment and authorized/escorted visitors, as determined by senior management within the operations group. Review of access controls and logs are conducted on a periodic basis to ensure compliance with business need to know/least privilege policy. Staff access to all company facilities is restricted by card key access.

Note: In October 2012, Visa initiated a program to migrate all of the CyberSource applications out of the subservicers providing co-location facilities in California and Colorado, and move them into the Visa data centers located in Highlands Ranch, CO – Operations Center Central (OCC) and Ashburn, VA – Operations Center East (OCE). Visa's OCC data center is the primary site while OCE is the secondary

site. The migration of production systems from the Equinix production data center to the Visa OCE data center was completed in the summer of 2014. The migration of production systems from the XO Communications data center was completed in fall of 2014. The co-location facilities in California and Colorado were then fully decommissioned in spring of 2015.

Physical Security in Visa's OCC and OCE Data Centers

Physical access to Visa's Operations Center East (OCE) and Operations Center Central (OCC) facilities is restricted to authorized individuals only. The OCE and OCC facilities are freestanding structures, occupied solely by Visa. Access/egress is limited to a single entry point, all exterior sides of each building are equipped with CCTV cameras, and all doors are equipped with CCTV cameras and intrusion-detection alarms. The OCC North Data Center is constructed with no exposure to exterior walls or windows. The OCC South Data Center and OCE Data Center PODs are exposed to exterior walls but not windows. A clear zone around each facility restricts parking and vehicle access.

There are guard stations at the main entrance of the OCE and OCC facilities to ensure that only authorized personnel are permitted access. Each building has uniformed security personnel onsite 24 hours per day, 365 days per year to monitor and control physical access. Electronic card access and video surveillance systems are used by the guard service to control and monitor access to the facility and to other sensitive areas. Access to Data Center operational areas is further restricted to personnel with an operational need for access.

All facility visitors must register at the reception desk and wear temporary visitor badges. Visa personnel must approve visitor access. Visa employees must wear photo identification badges. Visa Management must approve all employee, vendor, and non-employee requests for Visa photo identification badges. In addition, where legal and available, all employees, vendors, and other non-employees who require unescorted access to Visa's Data Centers must undergo criminal background checks.

Visa Management responsible for the specific secured area and the user's manager must approve card-key access levels. Access to Data Center floors is controlled using single-person access-control portals. Access is granted through these portals after both visual and electronic verification of the badge holder. Biometric devices are also used to control access to the OCE and OCC Data Centers.

The Visa Global Security Department maintains the card-key database. Only authorized personnel within the Visa Global Security Department may make changes to the card-key database and user access levels. Card-key access requests to sensitive areas must be documented and approved by an appropriate level of management.

All computer, telephony, and network equipment supporting the actual data center and tape libraries are housed within rooms that are controlled through the card-key system. Access to each room is restricted to authorized personnel who require access to perform their job responsibilities.

Physical security reviews are conducted annually at each Data Center, and problems or issues are brought to the attention of the appropriate Data Center Manager(s).

Terminated employees are required to return all card-keys and identification badges to their Manager upon termination.

Physical Environment

Environmental controls have been established to protect all of Visa's computer rooms, computer equipment, and tape libraries, including:

- Air conditioning system.
- Heat, smoke, and fire detectors.
- Water detectors.
- Raised flooring.

- Fire extinguishing system.
- Temperature and humidity sensors.
- Uninterruptible power supply (UPS) and diesel generators have been installed to protect Visa's facilities and computer equipment from a disruption in electrical power supply.
- Building management system to monitor the function and status of environmental control units.

All environmental control devices and UPS backup equipment are tested on at least an annual basis. Maintenance of computer hardware and peripheral equipment is performed on a periodic basis and is monitored by U.S.-based Central Facilities Support personnel.

Production Systems

Controls which refer to in-scope production systems refer to the following systems for both CyberSource Enterprise and Authorize.net (Small Business):

- Global Payment Processing Gateway (GPPG)
- Transaction Processing
- Enterprise Business Center (EBC)
- ConfigDB
- SuperUser2 (SU2)
- Mint (Merchant Interface)
- Rint (Reseller Interface)
- Decision Manager (DM)
- Fraud Detection System (FDS)
- Internal Fraud Tool (IFT)

CyberSource production applications run on Linux and Windows servers.

Data Backup

All critical systems are backed up on a regular basis using automated backup systems to support the completeness and accuracy of backup data. The following is a summary of the current backup policy.

- **Operating System:**
  - Monthly and weekly full backups with daily incremental backups
  - Retention period: up to seven years
- **Databases (Transactional):**
  - Daily full backups
  - Electronic Offsite replication at application server level
  - Retention period: up to seven years (of the backup from the last week of the month)
- **Database (Post transactional Reporting):**
  - Weekly full backups
  - Retention period: up to seven years

Incident Management

Incident management is used to document, track, and fix issues impacting the CyberSource environment. It provides oversight and a process involving incident owners and assignees. Processes for incident initiation, escalation, and resolution are documented.

CyberSource uses the Remedy Incident management system (also known as "VIPER") to record, track, and report issues affecting normal service operation. The group submitting the Incident Record is designated as the owner and assignee by system automation default, but the submitter may reassign ownership and assignment, as appropriate. Each incident is assigned an "impact" and "urgency" which controls the priority of the incident. Impact and urgency levels correspond to the impact or potential impact on CyberSource services. Priority levels are grouped into four categories:

Critical: Bridge in progress; Incident to be updated regularly to record new status; 24x7 resource commitment until resolved.

- Actual or highly probable service-level miss.
- Facility or critical component failure.
- Module or critical component failure
- Business or service function unavailable.
- Major customer impact.

High: Record should be updated daily until resolved; Resource commitment during normal business hours until resolved (24x7 for those groups that are 24x7)

- Possible Service level miss
- Application unavailable
- Widespread customer impact

Medium: Record should be updated along with resource commitment during regular business hours until a resolution is in place.

- Service impact but no service-level miss.
- Preventable business or service function incidents.

Low: Record should be updated when there is a new status to report. Resource commitment is to address any outstanding issues until a resolution is in place.

- Minimal impact to customer or service.

Incidents are placed in a *resolved status* once service operation has been restored. Incidents are *closed* when the resolution has been validated.

Problem Management

Problem management is used when incidents or issues become chronic or recurring; it is used to manage problem investigations and root cause analyses. It initiates actions taken to help prevent the reoccurrence of problems.

After a problem investigation identifies a cause (or mitigating factors) that information can be tracked and referenced going forward as either a known error or a solution database entry. A known error is a problem that has been successfully diagnosed and for which a temporary workaround or permanent solution has been identified. A solution database entry contains information that can be used to repair or restore a service.

Problem Management Policies, Procedures and responsibilities for identifying and escalating problems in the production environment have been established and are documented. Remedy (also known as "VIPER") is the problem management system used globally by CyberSource.

Logical Security Controls

Security Policies and Procedures

The Information Security department, under the responsibility of the Chief Information Security Officer, is responsible for administering security over the company's computer systems.

Visa's Global Information Security Policy, Objectives, and Standards are represented by the Visa Inc. Key Controls. Based on international standards ISO27000, the Key Controls are regularly reviewed and updated to align to industry best practices. The Key Controls define requirements for the protection of Visa information and other corporate information technology (IT) assets. Visa's Information Security Policy is owned by the Chief Information Security Officer, reviewed annually, and communicated to all Visa employees.

Management provides oversight and approval for exceptions to the Visa Key Controls utilizing a team of participants from Enterprise Risk and Information Security to perform ongoing administration (includes periodic changes and updates) of all components to the Visa Key Controls. This includes addressing noncompliance or violations with Visa Key Controls through existing policies and procedures to ensure corrective measures are completed on a timely basis.

Visa operates a vulnerability scanning program within the Attack Surface Management function which includes scanning of all IPs in the Visa network. Internal vulnerability scanning is conducted at least weekly for selected network devices and selected application servers for which resulting issues are monitored by management. Leveraging an industry accepted vulnerability scoring framework, issues are assigned severity ratings (Critical, High, Medium, etc.) and remediated in a prioritized manner or reviewed for engagement with governance bodies. Identified issues by the internal vulnerability scanning is reported to the Technology Leadership Team (TLT) on a weekly basis for review and follow up. In addition, a coverage analysis is performed quarterly to identify gaps in the vulnerability scanning coverage. Identified coverage gaps are resolved timely by management.

Penetration tests are conducted from both internal and external sources to evaluate certain Visa infrastructure, applications, and services at least annually and resulting issues are monitored by management and centrally tracked to resolution.

Defined policies include the usage of encryption techniques to protect user authentication information and remote access sessions over the internet. Electronic transmission of information between Visa and any other individual(s) or organization(s) is secured based on information classification to prevent unauthorized access to Visa computers, networks, and data. Inbound and outbound network connections between a Visa facility and an external network or computer are routed through a firewall or other approved network access control system expressly established to provide secure network access. Visa utilizes hardware security modules (HSM) and similar tamper resistant devices to perform encryption and decryption, providing an end to end encryption process that is intact from the point of data entry to the final system destination where decryption and/or authentication takes place.

Technical Security Requirements (TSR) are platform specific security requirements that aid in configuring Visa technologies to adhere to and support the enforcement of the Visa Key Controls. These formalized policies define and establish the minimum baseline security configurations covering areas such as user and group access security, file and directory security, restricted services, system update and installation standards and installed security software. In addition to the requirements specified in these policies, other security requirements may also apply depending on the type and specific technology implemented. Ensuring compliance to the TSRs are performed by the Visa Information Security team using the Qualys Policy Compliance tool. Management reviews, at least annually, existing Technical Security Requirement (TSR) policies to verify that system configuration standards are consistent with industry accepted hardening standards and to consider the need for additional TSRs. Management also provides oversight and approval for exceptions to against the Technical Security Requirements (TSRs).

Visa's Incident management program includes appropriate incident management responsibilities and procedures to ensure quick, effective, and orderly identification, response, and reporting of security incidents. The program and its associated runbooks are reviewed by external entities to ensure that recommended, leading practices are maintained. The program is tied into Visa's larger crisis

management program and plans for both are exercised on a regular basis, with additional Visa teams including, but not limited to Legal, Compliance, and Product Lines (amongst other entities). Legal and Compliance ensure that appropriate notification is made if an incident was to affect partner or customer records.

The CyberSource information security program is designed to safeguard information assets against unauthorized use, disclosure, modification, damage or loss and aligns with Visa Key Controls (Visa's global information security objectives and standards). The program incorporates education, policy review and development, technical security measures, and mechanisms to promote timely discovery and appropriate response to vulnerabilities and exploits. CyberSource adheres to security, availability, and privacy policies that have been approved by management and published and communicated to all employees. The security policies detail security objectives and measures and emphasize the importance of security to the business. Periodic updates to security policies and procedures are performed in a controlled fashion that includes reviews, approvals and revision tracking.

Security policies and standards are communicated to personnel via Key Controls training as well as the specific training associated with technologies and platforms. There is ongoing security and awareness training and education including annual key controls and acceptable use of computer resources training refresher.

Network Controls

CyberSource employs fully redundant, multi-tiered, network architecture. Network subnets are protected by firewalls with granular access lists that limit services to only those necessary for the application layer to function. Only authorized employees utilizing unique user IDs and passwords have the ability to manage firewall rule sets. Environments for software development, integration testing, quality assurance testing, user acceptance testing and production are logically and/or physically separated. To provide the highest level of security for sensitive customer data, CyberSource network policy requires all application traffic traversing the Internet to do so through an encrypted channel. Furthermore, all hosts that store personal account number data employ data encryption, and most employ host based firewalls as part of a "defense-in-depth" strategy.

CyberSource has implemented logical security control policies that limit access to systems, devices and applications to the level justified by business need and job responsibility. Upon termination, access is removed in a timely manner. Remote access to CyberSource's networks is restricted based on job responsibility and is limited to personnel with a business need. Such access occurs over an encrypted virtual private network (VPN) and requires multifactor authentication. Passwords are required to be complex and periodically changed. Management reviews access to production systems periodically to determine the appropriateness of access.

Detective controls are used extensively to provide both real time monitoring and auditing of the environment to ensure compliance with CyberSource information security policies. Such controls include regular vulnerability scanning, penetration testing, IDS, file integrity monitoring and other audit logging and review procedures. Vulnerability assessment and remediation is performed regularly to help ensure that Internet accessible services are protected from known security exploits. Access to related sensitive supporting systems is limited to appropriate personnel based on job responsibility and need to know/least privilege access control.

Change Management

Change Management Policies and Procedures have been established and documented for customary and emergency changes into the production environment.

The Process team provides monitoring, reporting, and escalation of records that do not meet the appropriate process criteria.

The appropriate systems software group will evaluate the nature of each change, prepare a test plan, and test the change on the lab and development systems. The change will then be tested for a period of time

(depending on the nature of the change) on the test system. Once the appropriate groups are satisfied that the change has been adequately tested and evaluated, the change will follow the customary change control process, and it will be discussed during the semi-weekly change control meeting.

When pre-implementation testing of a change is required, the support, development, or QA group facilitating the change for that particular system will retain test results associated with the change.

Remedy is Visa's system of record for all changes to production environments. The Remedy tool and related process is collectively known as VIPER and facilitates the change control process. It provides monitoring and tracking for the activities noted within the records. The process requires that changes are moved into production with the appropriate levels of review, oversight, and approval. Change request tickets in the VIPER system require approvals before they can be implemented and closed. Change request tickets have many required fields which include: summary, risk level, timing, business justification, service impact assessment, back-out plan, install plan, and escalation information. Additionally, information detailing the change request can be found in the work Detail Items within the change record. VIPER has systematic controls that enforce the completion of these fields before a ticket can be submitted for approval.

Approval Process

The approval requirements for each change are automatically assigned by the system based on approval workflows (or paths) that have been input into VIPER. The system assigns the designated approval path based on the classification of change (e.g. application, operating system, database, etc.) and other factors such as the criticality and location. The approvers within the approval groups maintained in the VIPER system are reviewed by management annually for appropriateness.

Approvers are automatically notified by VIPER of pending approvals via system e-mails generated when an approval is required for a change. Required approvals per system rules vary depending on the change type. As an example the approvers for a software or application change include Application Development, Infrastructure Support, QA, Change Manager and assignee group. Additionally, the VIPER system is configured such that the ticket submitter is not able to approve their own ticket even if they are a member of an approver group and are included in the approver list. Additional approvals may be added to a particular ticket at the request of the change business owner.

The QA approval is considered evidence that the required testing is complete for a particular change except for hardware and database changes, as they do not require QA approval due to the nature of the change.

Changes cannot reach the implementation schedule unless all approvals (as defined by VIPER) are obtained.

Change Categories

There are five categories of changes: Normal, Expedited, Standard Preapproved, Emergency and Latent.

1. The Normal change category has a minimum lead time of 7 days for a change to be submitted prior to its scheduled start date and time. The change must be moved forward to the scheduled for approval stage at least 7 days prior to the scheduled start date and time giving approvers ample time to review and approve the request.
2. The Expedited change category has a start date window that must be less than 7 days of ticket creation and have a timing reason for the change. If the scheduled start date is more than 7 days of ticket creation, the change cannot be classified as Expedited. Expedited changes are considered the same as normal changes with a shorter lead time for approvals prior to implementation. A timing reason is required to provide sufficient background and rationale to support the need of an Expedited change. Sr. Manager and Executive Manager approvals are added to expedited changes.

3. A Standard Preapproved Change (SPC) is approved once by the executive change advisory board and may be implemented multiple times through the use of an SPC template within the VIPER system. Once the SPC has been board approved, the implementation iterations are documented, scheduled and tracked. SPC's undergo a yearly review to determine if they continue to meet the requirements to be classified as an SPC.
4. The Emergency change category has a start date window that must be within 36 hours of ticket creation and have a timing reason for the change. If the scheduled start date is more than 36 hours of ticket creation, the change cannot be classified as Emergency. Due to the nature of emergency changes, Emergency changes are approved by the assignee group prior to implementation and post approved by all other groups after implementation. The submitter's direct manager is added as an approver on emergency changes.
5. The Latent change category is a change that has to be conducted immediately due to a critical failure where there is not sufficient time to open a change record prior to taking corrective action. The latent change is opened post implementation and enters the completed stage once submitted. All approval groups must approve the change record before the record can be closed. The submitter's direct manager is added as an approver on latent changes.

Transactional Controls

Transaction fees are automatically calculated on a monthly basis based on transaction volume and established pricing. Program changes to transaction fee calculation are documented, tested, and approved prior to migration to production. Access to update established pricing tables is restricted to appropriate personnel. Updates to established pricing tables are documented and approved. A monthly analytic review is performed on customer activities, billable transactions and quotes information.

Control Objectives and Related Controls

CyberSource's control objectives and related controls are included in Section 4, Control Objectives, Related Controls, and Tests of Operating Effectiveness of this report to eliminate the redundancy that would result from listing them in Section 3 and repeating them again in Section 4. Although the control objectives and related controls are included in Section 4, they are nevertheless an integral part of CyberSource's description of controls.

Complementary Client Organization Controls

CyberSource services were designed with the assumption that certain complementary client organization controls would be implemented by client organizations (i.e., merchants, and resellers). This section describes those additional policies, procedures, and controls that should be in operation at any CyberSource client organization to complement the service and corresponding controls. Client organizations' auditors should consider whether the following controls have been placed in operation at the client organization. Client organizations responsibilities include, but are not limited to, the following:

- **Control Objective 6: Logical Security**

  The application of the following complementary client controls by client organizations is necessary to achieve Logical Security control objective described in Section 4:

  - The client is responsible for user administration:
    - Adding and removing authorized users for its account
    - Establishing and assigning user permissions / rights
    - Establishing and administering segregation of duties
  - The client is responsible for changing the merchant administrative password provided with the initial application setup.
  - The client is responsible for ensuring browser compatibility with 128 bit encryption.
  - The client is responsible for periodically generating and implementing new authentication/encryption keys as described in CyberSource's documentation.
  - The client is responsible for deploying and maintaining adequate malware protection controls at endpoints which connect to the CyberSource environment.
  - The client is responsible for revalidation of user access to the CyberSource environment on a periodic basis (i.e., user access review).
  - The client is responsible for ensuring that passwords used within their environments are sufficient to their requirements.
  - The client is responsible for ensuring that monitoring and logging controls (e.g. events, user activities, etc.) are in place within their environment.

- **Control Objective 9: Transactional Controls**

  Each client should establish its own business controls to ensure processing integrity, including transaction authentication and authorization; processing completeness and accuracy; and data completeness, accuracy, and integrity. The application of following complementary client controls by client organizations is necessary to achieve Transactional Controls control objective described in Section 4:

  - The client is responsible for configuring and using the services as set forth in the relevant CyberSource documentation.
  - The client is responsible for establishing and complying with all requirements for application interfaces, including the completeness and accuracy of information.
  - The client is responsible for maintaining third party relationships with other service providers that may be involved in the transaction processing flow, e.g., the merchant's bank and the merchant acquirer.

- The client is responsible for the completeness and integrity of data that is transmitted to CyberSource for processing.
- The client is responsible for reviewing the accuracy and completeness of their transaction volume used for processing and invoicing by CyberSource.
- The client is responsible for ensuring any pricing updates have been correctly reflected in the periodic and regular billings received from CyberSource.
- The client is responsible for monitoring and ensuring their compliance with all applicable laws, regulations, or other governmental and industry requirements for security, corporate governance, privacy, etc.

The list of complementary client organization control considerations presented above does not represent a comprehensive set of all the controls that should be employed by client organizations. Other controls may be required at client organizations.

Description of Services Provided by Subservice Organizations

CyberSource has contracted with the third party subservice organizations listed below, for peering points and protocol conversions. This report addresses only those controls and related control objectives of CyberSource, as detailed under Section 4, and does not include controls and related control objectives of the subservice organizations noted below.

Subservice Organizations	Location	Service Role
XO Communications Internap	Colorado	Peering point from October 1, 2014 to January 25, 2015. Production systems housed in Visa Facility thereafter.
Internap Savvis	England	Peering point and protocol conversion

Background

This section includes KPMG LLP's ("KPMG") tests of operating effectiveness. The control objectives and related control descriptions placed in operation have been provided by CyberSource and form an integral part of their description of controls.

Organizational Management

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 1 Organizational Management *Controls provide reasonable assurance that personnel policies and procedures regarding employee hiring and training are in place.*		
1.1 Information security policies and procedures are documented and communicated to new hires.	Inquired of management to obtain an understanding of how information security policies and procedures are documented and communicated to new hires. Inspected Visa Global Compliance documentation and Visa Key Controls to determine whether information security policies and procedures are documented and are available for reference to new hires. Refer to **Organizational Management 1.2, 1.4,** and **1.6** below for tests of operating effectiveness related to training and the acknowledgement and receipt of the understanding of information security policies and procedures.	No exceptions noted.
1.2 New employees are required to sign a Proprietary Information Agreement which states that employees agree to uphold company privacy and confidentiality policies. Human Resources maintain the signed copies of the agreement within employee files.	Inquired of management to obtain an understanding of the requirements documented in the proprietary Information agreement and the process to obtain signatures for each new employee. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether new employees are required to sign the Proprietary Information Agreement (PIA). Inspected the Proprietary Information Agreements of a selection of new hires to determine whether new hires signed the propriety information agreement.	No exceptions noted.
1.3 Background investigations for new employees are completed prior to start date.	Inquired of management to obtain an understanding of the background investigation process in place. Inspected policy documentation to obtain an understanding of the background investigation process in place to determine whether the process defined was consistent with inquiry. Inspected third party background investigations system and badging system for a selection of new hired employees and contractors to	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 1 Organizational Management *Controls provide reasonable assurance that personnel policies and procedures regarding employee hiring and training are in place.*		
	determine whether for each employee background checks were completed prior to the employees' start date and issuing the permanent photo identification badge.	
1.4 Employees are required to complete the online Visa Corporate Key Controls training within 45 days of new employment and annually thereafter. If training is not completed within the 45 day requirement, management performs follow-up and escalates as needed.	Inquired of management to obtain an understanding of the process used to manage the online Visa Corporate Key Controls training for new employees and annual renewals. Inspected the Visa Global Compliance documentation to determine whether the process of completing the online Visa Corporate Key Controls training for new employees and annual renewals are defined. Inspected training certificates for a selection of new hires and existing employees (full-time employees and contractors) to determine whether the employees completed the online Visa Corporate Key Controls training within 45 days of joining and annually thereafter. Inspected escalation documentation for a selection of employees to determine whether follow ups and escalations were performed by management for any delays in completing the training within 45 days.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 1 Organizational Management *Controls provide reasonable assurance that personnel policies and procedures regarding employee hiring and training are in place.*		
1.5 Employees are required to complete the Visa Code of Business Conduct and Ethics training within 45 days of new employment and annually thereafter. If training is not completed within the 45 day requirement, management follows up and escalates as needed.	Inquired of management to obtain an understanding of the process of managing the online Visa Inc. Code of Business Conduct and Ethics training for new employees and annual renewals. Inspected the Visa Global Compliance policy documentation to determine whether policies were defined where employees are required to complete the online Visa Inc. Code of Business Conduct and Ethics training within 45 days of joining and annually thereafter Inspected training certificates for a selection of new hires and existing employees (full-time employees and contractors) to determine whether the employees completed the online Visa Corporate Code of Business and Ethics training within 45 days of joining and annually thereafter. Inspected escalation documentation for a selection of employees to determine whether follow ups and escalations were performed by management for any delays in completing the training within 45 days.	No exceptions noted.

Physical Access

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 2 – Physical Access *Control provide reasonable assurance that physical access to the data center computer facilities, equipment, storage media, and key security devices are restricted to authorized personnel.*		
Visa Controls for U.S. Visa Data Centers and Controls for Subservicer Data Center – Applicable to the XO Communications Data Center from October 1, 2014 to January 25, 2015		
2.1 Physical access policies and procedures have been established and documented.	Inspected the Global Security and Safety intranet website, Visa Inc. Key Controls, Policies & Procedures, and OCE badging Procedures to determine whether the documented physical access policies and procedures have been defined, were current, and accessible to all personnel by Visa's Intranet. Inspected Visa Inc. Key Controls, Policies & Procedures as well as the Global Security and Safety intranet website to determine whether documented physical access policies and procedures have been defined, were current, and accessible to all personnel by Visa's Intranet.	No exceptions noted.
2.2 Data center entry points are restricted through the following mechanisms: ▪ Proximity card access through a portal (or man trap) ▪ Monitoring by security staff and closed circuit television (CCTV)	Inquired of management to obtain an understanding of how the mechanisms in place restrict access to the data center. Observed the data center facilities to determine whether the proximity card reader systems were implemented to secure the building perimeter, controlled interior office space, data centers, and secure access zones. Inspected the following mechanisms to determine whether each of the following were in place: ▪ Biometrics reader does not work when presented with incorrect biometrics. ▪ Dual-occupancy enforcement mechanisms trigger an alarm when only one person is in the room. ▪ Special Access Zones (SAZ) have slab to slab constructions. ▪ CCTVs monitor SAZ entrances and exits.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 2 – Physical Access *Control provide reasonable assurance that physical access to the data center computer facilities, equipment, storage media, and key security devices are restricted to authorized personnel.*		
2.3 Access to make changes to the proximity card reader system is restricted to authorized individuals.	Inquired of management to obtain an understanding of how access to make changes to the proximity card reader system is restricted to authorized individuals. Inspected HR documentation and the complete list of individuals with access to make changes to the proximity card reader system, to determine whether the access was restricted to a limited number of authorized personnel, based on job responsibilities.	Exceptions noted. Of a full population of 22 employees with access to make changes to the proximity card reader, KPMG noted that 3 employees on the list had been terminated in 2013-2014 and still retained inappropriate access to the card reader system. KPMG inspected evidence and noted that none of the employees had made changes to the system after their respective termination dates. **Management Response:** Management attributed the exception to human error for having missed removing the terminated users' accounts, within this specific application tool, in a timely manner. The users' network accounts, which are required to access the system, were disabled at the time of termination. Once the exception was discovered, the identified users were immediately removed from this application tool and, as noted by KPMG, confirmed there were no unauthorized changes after the respective termination dates. Beginning in October 2015, management implemented a monthly review to validate users with access to this specific application tool which will identify terminated personnel to be removed more timely. Management asserts that the issue is remediated.
2.4 Physical access to the data centers is authorized by management and access to secured areas is authorized by room managers.	Inquired of management to obtain an understanding of how the physical access to the data center must be authorized by management and access to secured areas must be authorized by room managers. Inspected the Global Security and Safety intranet website and badging procedures document to determine whether the physical access to the data centers and secured areas	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 2 – Physical Access *Control provide reasonable assurance that physical access to the data center computer facilities, equipment, storage media, and key security devices are restricted to authorized personnel.*		
	must be authorized, and correspond to the access procedures described by management. Inspected documentation for a selection of users whose access was provisioned to data centers and secured areas to determine whether the access was authorized by management and room managers.	
2.5 Physical access to the data centers and secured areas is revoked upon termination or transfer.	Inquired of management to obtain an understanding of how the physical access to the data centers and secured areas is revoked in a timely manner upon termination or transfer. Inspected badging and termination procedures to determine whether the procedures to remove access to the data centers were consistent with management's description. Inspected access revocation evidence for a selection of terminated employees and contractors to determine whether the physical access to the data centers and secured areas was revoked upon termination or transfer.	Exceptions noted. Of a selection of 40 terminated employees, KPMG determined that 1 employee did not have their badge revoked in a timely manner and was revoked two days after the termination date in August 2015. KPMG further noted that the badge was used 1 day after termination in the general office area. **Management Response:** Management attributed the exception to not having collected the terminated employee's building access badge in a timely manner. Although the Human Resource (HR) termination request to deactivate the building access was submitted timely, the badging system was undergoing scheduled maintenance for which the deactivation was not processed until the next business day. Management asserts that the general office area is a low risk area with no sensitive assets and that the terminated employee came onsite for a meeting with a current employee when the unauthorized access occurred. As a result of this exception, HR updated the formal Manager Checklist – Exiting Employee document to clarify and explicitly state that the direct manager is responsible for collecting the building access badges of their employees upon termination. Management asserts that the issue is remediated.

Control Description	Test Performed	Test Results
Control Objective No. 2 – Physical Access *Control provide reasonable assurance that physical access to the data center computer facilities, equipment, storage media, and key security devices are restricted to authorized personnel.*		
2.6 Visitors are required to present identification and are escorted when required.	Inquired of management to obtain an understanding of how the visitors were required to present identification and were escorted when required. Observed the data center facilities to determine whether visitors were required to present identification and were escorted when required.	No exceptions noted.
2.7 Guard service policies and procedures have been established and documented. A physical access incident log is maintained and timely action is taken when physical security incidents occur, including proper notification of data center management.	Inquired of management to obtain an understanding of how the guard service policies and procedures have been established and documented and how the physical access incident log is maintained. Inspected the guard service policies and procedures to determine whether it contained guidelines for guard service and incident reporting. Inspected incident reports for a selection of data center physical access incidents (event logs) to determine whether timely action was taken when physical security incidents occurred, including proper notification of data center management.	No exceptions noted.
2.8 Closed Circuit Television (CCTV) cameras are installed at entrances, exit doors, emergency doors, and sensitive areas. The cameras have uninterruptible power supplies or a backup power source and are capable of providing continuous recording of video. The recorded video is retained for a minimum of 45 days.	Inquired of management to obtain an understanding of how the Closed Circuit Television (CCTV) cameras were installed at entrances, exit doors, emergency doors, and sensitive areas. The cameras have uninterruptible power supplies or a backup power source and were capable of providing continuous recording of video. The recorded video is retained for a variable amount of time dependent on disk space. Observed the data centers to determine whether the Closed Circuit Television (CCTV) cameras were installed at entrances, exit doors, emergency doors, and sensitive areas at the data center. Inspected a selection of video screenshots from 45 days prior to the request date to determine whether the recorded video was retained for 45 days or more.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 2 – Physical Access *Control provide reasonable assurance that physical access to the data center computer facilities, equipment, storage media, and key security devices are restricted to authorized personnel.*		
2.9 A physical security site survey is conducted on an annual basis and management follow-up is required on identified observations.	Inquired of management to obtain an understanding of how a physical security site survey is conducted on an annual basis and management follow-up is required on identified observations. Inspected the Visa Data Center Security Standards to obtain an understanding of the timeliness and parties responsible for Visa annual data center reviews. Inspected the annual Physical Security Compliance and Risk Review reports for data centers to determine whether a physical security site survey is conducted on an annual basis and management follow-up was performed on identified observations.	No exceptions noted.
2.10 Access doors and other access methods are alarmed with intrusion detection systems. Exiting from an emergency door activates an alarm and security takes action on the alarm.	Inquired of management to obtain an understanding of mechanisms in place to enforce intrusion and emergency door alarms. Observe mechanisms at the facilities to determine whether the expected alarms were triggered when emergency doors were opened.	No exceptions noted.
2.11 Management reviews the data center room report at least monthly to ensure access is appropriate. If access is inappropriate, access is modified.	Inquired of management to obtain an understanding of mechanisms in place to ensure management reviews data center room reports at least monthly to determine whether access was appropriate and, if not, access was modified. Inspected the Badging Office Procedures to determine whether the documented process for reviewing the data center room report is consistent with management's description. Inspected data center room reports for a selection of months and room owners to determine whether the management review was conducted and corresponding user modifications were performed.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 2 – Physical Access *Control provide reasonable assurance that physical access to the data center computer facilities, equipment, storage media, and key security devices are restricted to authorized personnel.*		
2.12 Photo identification is not issued until the employee's background investigation is completed.	Inquired of management to obtain an understanding of how the permanent photo identification is not issued until the employee's background investigation is completed. Inspected the badging Office Procedures to determine whether the documented process for issuing photo identification upon completion of background investigation is consistent with management's description. Inspected third party background investigations system and badging system for a selection of new hired employees and contractors to determine whether for each employee background checks were completed prior to the employees' start date and prior to issuance of the permanent photo identification badge.	No exceptions noted.

Physical Environment

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 3 Physical Environment *Controls provide reasonable assurance that IT facilities, equipment, and storage media at the data centers are protected from damage resulting from environmental conditions.*		
Visa Controls for U.S. Visa Data Centers and Controls for Subservicer Data Center – Applicable to the XO Communications Data Center from October 1, 2014 to January 25, 2015		
3.1 Environmental systems have been implemented such that the data centers are protected from environmental hazards, including: ▪ Heat, smoke and water detectors; ▪ Fire control system; ▪ Temperature and humidity control equipment; and ▪ Power management system including UPS and generators.	Inquired of management to obtain an understanding of the mechanisms implemented to protect data centers from environmental hazards. Inspected environmental hazards policies and procedures to determine whether documented procedures were defined and consistent with management's description. Performed a walkthrough of the data centers to observe that environmental systems have been implemented such that the data centers were protected from environmental hazards, including: ▪ Heat, smoke and water detectors; ▪ Fire control system; ▪ Temperature and humidity control equipment; and ▪ Power management system including UPS and generators.	No exceptions noted.
3.2 Environmental equipment is continuously monitored and service is scheduled as needed. When maintenance issues arise, change and problem records are opened and the issue is managed through completion.	Inquired of management to obtain an understanding of whether the environmental equipment is continuously monitored and service is scheduled as needed. When maintenance issues arise, change and problem records were opened and the issue is documented through completion. Inspected the preventive maintenance guidelines for environmental equipment to determine whether maintenance guidelines were documented and updated / reviewed on a periodic basis.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 3 Physical Environment *Controls provide reasonable assurance that IT facilities, equipment, and storage media at the data centers are protected from damage resulting from environmental conditions.*		
3.3 Environmental equipment is continuously monitored and service is scheduled as needed. When maintenance issues arise, change and problem records are opened and the issue is managed through completion.	Inquired of management to obtain an understanding of whether the environmental equipment is continuously monitored and service is scheduled as needed. When maintenance issues arise, change and problem records were opened and the issue is documented through completion. Refer to **Problem Management 5.4** on page **4-15** and **Change Management 7.3** on page **4-25** for tests of operating effectiveness related to the problem management and change management processes respectively.	No exceptions noted.

Backup and Recovery

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 4 Backup and Recovery *Controls provide reasonable assurance that computer systems are backed up to storage media on a periodic basis and that procedures are employed to maintain the integrity of the storage media.*		
4.1 Backup policies, procedures, and responsibilities have been established and documented.	Inquired of management to obtain an understanding of the backup policies, procedures, and responsibilities that have been established and documented. Inspected the backup policies, procedures, and responsibilities to determine whether they have been established and documented.	No exceptions noted.
4.2 Replication of production databases/data to backup data centers are performed using automated systems.	Inquired of management to obtain an understanding of the process of replicating production data to backup systems. Inspected CyberSource Production Database Replication Design Diagram to determine whether production databases/data are designed to replicated to backup data centers Inspected the data replication configurations for CyberSource systems to determine whether production databases/data are replicated to backup data centers and that failures or errors during the replication process results in an alert and /or incident.	No exceptions noted.
4.3 System checks and automated tools are utilized to ensure the completeness and accuracy (integrity) of the replicated data.	Inquired of management to obtain an understanding of the process of performing system checks using an automated tool to ensure the completeness and accuracy of the data replication and integrity process. Inspected data integrity and replication configurations within the automated tool for a selection of CyberSource databases to determine whether an automated tool was utilized to ensure the completeness and accuracy of the data prior to replication. Inspected the most recent results of the automated tool (including the associated VIPER tickets) for a selection of CyberSource databases to determine whether a comparison integrity check was performed during the period.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 4 Backup and Recovery *Controls provide reasonable assurance that computer systems are backed up to storage media on a periodic basis and that procedures are employed to maintain the integrity of the storage media.*		
4.4 Information security risk reports are provided to management quarterly to identify and address potential operational disruptions, system availability and data compromises which could impair system security commitments.	Inquired of management to obtain an understanding of the information security risk reports provided to management on a quarterly basis. Inspected documentation for a selection of quarterly reports submitted to management to determine whether they identify and address potential operational disruptions, system availability and data compromises which could impair system security commitments.	No exceptions noted.

Problem Management

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 5 – Problem Management *Controls provide reasonable assurance that system problems are properly recorded, analyzed, and resolved in a timely manner.*		
5.1 Incident management policies and procedures for identifying and escalating problems in the production environment have been established and documented.	Inspected problem management documentation to determine whether formal policies and procedures have been defined, are current, available from Visa's Intranet, and reviewed and updated by management on a periodic basis.	No exceptions noted.
5.2 An incident management system is in place to record, track, and monitor identified problems.	Inquired of management to obtain an understanding of whether an incident management system was in place to record, track, and resolve identified problems in the production environment. Observed the BMC Remedy system during walkthrough to determine whether the BMC Remedy System existed and was used to record, track, and resolve and escalate incidents/ problems identified in the production environment.	No exceptions noted.
5.3 Production systems are monitored by Operations staff 24/7/365.	Inquired of management to obtain an understanding of the process of monitoring production systems. Inspected the Operations daily schedules for a selection of days to determine whether formal shift definitions exist with personnel assigned to each shift, and that production systems were monitored by operations staff daily. Inspected the Network Operation schedule to determine whether the current schedules are designed to monitor the production systems 24/7/365.	No exceptions noted.
5.4 Identified incidents are resolved and closed in a timely manner in accordance with policies and procedures (in line with internal Service Level Agreements – SLAs).	Inquired of management to obtain an understanding of how incidents were resolved and closed in a timely manner and in accordance with policies and procedures. Inspected the Visa Global Incident Management Process framework policy documentation to determine whether it defines the process for incident resolution.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 5 – Problem Management *Controls provide reasonable assurance that system problems are properly recorded, analyzed, and resolved in a timely manner.*		
	Inspected documentation for a selection of incident records to determine whether reported incidents were resolved and closed in a timely manner in accordance with policies and procedures.	
5.5 Incident aging reports are generated and distributed to managers on a monthly basis, at a minimum, to assist in timely incident resolution	Inquired of management to obtain an understanding of how incident aging reports were produced and reviewed by management on a weekly basis to assist in timely incident resolution. Inspected incident management policies and procedures documentation to determine whether the process to generate incident aging reports and review them on a weekly basis was documented and consistent with management's description. Inspected documentation for a selection of weekly incident aging reports to determine whether incident aging reports were reviewed by management on a weekly basis.	No exceptions noted.
5.6 Incident management reports are generated and distributed to managers on a monthly basis for their review to monitor timely incident resolution.	Inquired of management to obtain an understanding of how incident management reports were generated and distributed to managers at least monthly for their review to monitor timely incident resolution. Inspected incident management policies and procedures documentation to determine whether the process to generate incident management reports for distribution at least monthly was documented and consistent with management's description. Inspected incident management documentation for each incident report type to determine whether incident management reports were generated at least monthly and reviewed to monitor timely incident resolution.	No exceptions noted.

Logical Security

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
6.1 Multifactor authentication is required for remote access to production.	Inquired of management to obtain an understanding of how multifactor authentication is implemented for remote access to production. Inspected Visa Inc. Key Controls, Objectives and Standards documentation to determine whether multifactor authentication is required for remote access to production. Observed the process of authenticating to production systems to determine whether multifactor authentication is required for remote access to the production environment.	No exceptions noted.
6.2 Management reviews remote access to production systems annually to ensure that access is restricted to current employees with valid business purpose and job responsibilities that warrant access.	Inquired of management to obtain an understanding of the process of user validation of remote access to production systems conducted by management annually. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether periodic user access review is required. Inspected the data validation report used to identify the orphan IDs for a selection of user access reviews to determine whether orphan IDs were found and were removed timely upon identification. Inspected evidence of the annual user access review of remote access to production to determine whether management reviewed access to ensure that access was restricted to current employees with valid business purpose and job responsibilities that warrant access, and that any inappropriate access identified during the review was removed in a timely manner.	Exceptions noted. KPMG noted that a full Unix user access review was not performed during the examination period. **Management Response:** Management attributed the exception to a change in the access review process within the organization from needing to run multiple entitlement-based access reviews to fewer role-based access reviews which took longer to implement than expected. Management performed a UNIX privileged access review during the period of this audit but did not complete a full UNIX user access review. The full UNIX user access review was started in October 2015 and is scheduled to be completed in December 2015.
6.3 Management reviews internal access to client-portal applications annually to ensure that access is restricted to current	Inquired of management to obtain an understanding of the process of user validation	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
employees with valid business purpose and job responsibilities that warrant access.	of internal access to client-portal applications conducted by management annually. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether annual user access review is required. Inspected evidence from the annual user access review of internal access to client-portal applications to determine whether access was reviewed at least annually and that any inappropriate access identified during the review was removed.	
6.4 Access to the IDS logs is audited at a minimum semi-annually to validate that logs are restricted to appropriate personnel. If access is inappropriate, access modifications are made.	Inquired of management to obtain an understanding of the process of user access validation and remediation. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether periodic user access review is required. Inspected the semi-annual user access review of IDS log access within Checkpoint to determine whether management reviewed access to ensure that access is restricted to current employees with valid business purpose and job responsibilities that warrant access, and that any inappropriate access identified during the review was removed timely.	No exceptions noted.
6.5 Visa personnel monitor security alert bulletins and use an automated monitoring tool to monitor the deployment of relevant system patches on open systems to ensure that patches are installed on servers.	Inquired of management to obtain an understanding of whether Visa personnel monitor security alert bulletins and use an automated monitoring tool to monitor the deployment of relevant system patches on open systems to ensure that patches were installed on servers. Inspected documentation to determine whether policies and procedures for identification of security vulnerabilities and deployment of patches were formally documented. Inspected screenshots from the QualysGuard application to determine whether a compliance monitoring tool exists to identify and apply past due patches based on criticality of vulnerability. Refer to **Application Development and Change Management 7.3** on page **4-25** for	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
	tests of operating effectiveness related to testing of patch deployments. Refer to **Logical Security 6.17** on page **4-22** tests of operating effectiveness related to vulnerability scanning.	
6.6 Network passwords adhere to Visa's password and user ID policy requirements for the following attributes: · Password expiration; · Password length; · Password reuse; · User ID failed attempt lockout; and · User ID lockout duration.	Inquired of management to obtain an understanding of how passwords and user IDs used to access to CyberSource domain and the Authorize.Net domain are configured. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether it contains requirements on password attributes. Inspected the network password configurations to determine whether network passwords adhere to Visa's password and user ID policy requirements.	No exceptions noted.
6.7 Access to production systems is documented and authorized in accordance with policies and procedures.	Inquired of management to obtain an understanding of the relevant policies and procedures and how access request to production systems is documented and authorized. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether access to Visa systems, networks, application, and information must be approved by management and require that all requests be documented and retained. Inspected access requests for a selection of new users granted access to production systems to determine whether access was granted based on documented approval/authorization in accordance with policies and procedures.	No exceptions noted.
6.8 Terminated user access is removed from production systems.	Inquired of management to obtain an understanding of the process used to remove terminated user access from production systems. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether policy requires users with privileged access be suspended or disabled immediately and all remaining access must be removed or blocked within 30 days. Inspected access revocation evidence for a selection of terminated employees and	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
	contractors to determine whether the access to each system was revoked in a timely manner upon termination. Inspected the complete population of active user accounts for production systems and compared the list against the HR termination listing to determine whether no terminated users had access to production systems.	
6.9 Policies and procedures exist to address noncompliance or violations with Visa Key Controls and that corrective measures are performed on a timely basis.	Inspected policies and procedures to determine whether they have been established and documented to address noncompliance or violations with Visa Key Controls and that corrective measures are performed on a timely basis.	No exceptions noted.
6.10 Management provides oversight and approval for exceptions to the Visa Key Controls.	Inquired of management to obtain an understanding of oversight and approval process for exceptions to the Visa Key Controls. Inspected evidence of reviews performed to determine whether the reviews tracked and investigated non-compliance to Visa Key Controls. Inspected documentation presented to the Business Controls Working Group (BCWG) for review and approval for a selection of exceptions to determine whether an assessment was performed and consistent with documented process.	No exceptions noted.
6.11 A project management office team is responsible for managing and maintaining changes and performs quarterly updates to the Visa Key Controls.	Inquired of management to obtain an understanding of how the project management office team performs quarterly updates the Visa Key Controls. Inspected documentation for a selection of project management quarterly updates performed on Visa Key Controls to determine whether the project management office performs ongoing administration of the Visa Key Controls.	No exceptions noted.
6.12 Defined policies include the usage of encryption techniques to protect user authentication information and remote access sessions over the internet.	Inquired of management to obtain an understanding of whether defined policies include the usage of encryption techniques to protect user authentication information and remote access sessions over the Internet.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
	Inspected Visa Key Controls, Policies & Procedures to determine whether policies were defined for usage of encryption techniques.	
6.13 Technical Security Requirement (TSR) policies have been defined to establish the minimum baseline security configurations addressing: ▪ User and group access security ▪ File and directory security ▪ Restricted services ▪ System update and installation standards ▪ Installed security software	Inquired of management to obtain an understanding of how TSR policies have been defined to establish the minimum baseline security configurations. Inspected a selection of TSR policies to determine whether they have been defined to establish the minimum baseline security configurations consistent with control description.	No exceptions noted.
6.14 Management reviews, at least annually, existing Technical Security Requirement (TSR) policies to verify that system configuration standards are consistent with industry accepted hardening standards and to consider the need for additional TSRs.	Inquired with management to obtain an understanding of the annual review of the TSR policies. Inspected evidence of review for a selection of TSR policies to determine whether the review was performed consistent with the control description and inquiry. Inspected the meeting minutes of the annual GIS meeting to determine whether the TSR policies were reviewed and whether any updates were made.	No exceptions noted.
6.15 Management uses automated tools to monitor system configurations for compliance against the Technical Security Requirements (TSRs).	Inquired with management to obtain an understanding of the automated tools used to monitor system configurations for compliance against the Technical Security Requirements (TSRs). Inspected system configuration to determine whether automated tools are used to monitor system configurations for compliance against the Technical Security Requirements (TSRs). Inspected evidence of the TSR Ticketing data flow and incident ticket created in the VIPER system to determine whether auto-ticketing process was in place to create tickets for scan findings. Inspected evidence of suppression details in Qualys for sample Suppression ID selected to determine whether the TSR approval was provided prior to suppression being performed and valid through the suppression period.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
	Inspected evidence of trending analysis for TSR compliance exceptions to determine whether compliance and count of open tickets were appropriate.	
6.16 Management provides oversight and approval for exceptions against the Technical Security Requirements (TSRs).	Inquired of management to obtain an understanding of the oversight and approval process for exceptions against the Technical Security Requirements (TSRs). Inspect evidence of reviews performed to determine whether the reviews tracked and investigated non-compliance to Technical Security Requirements (TSRs). Inspected documentation presented to management for review and approval for a selection of exceptions to determine whether an assessment was performed and consistent with documented process.	No exceptions noted:
6.17 Internal vulnerability scanning is conducted at least weekly for critical/high risk network devices and production servers and resulting issues are monitored by management. Leveraging an industry accepted vulnerability scoring framework, issues are assigned severity ratings and remediated in a prioritized manner or reviewed for engagement with governance bodies.	Inquired of management to obtain an understanding of whether internal vulnerability scanning was conducted at least weekly for network devices and production servers and the resulting issues were monitored by management. Inspected Visa Key Controls, Policies & Procedures to determine whether policies were defined for vulnerability scanning. Inspected the configuration of the vulnerability management scanning tool to determine whether it was configured to scan at least weekly. Inspected vulnerability scanning documentation for a selection of weeks to determine whether scanning was conducted at least weekly and whether resulting issues were monitored and resolved by management. Inspected documentation for a selection of vulnerability reports to determine whether vulnerabilities were assigned a priority level based on established framework. Inspected vulnerability scanning documentation to determine whether open critical and high vulnerabilities were remediated timely or reviewed with governance bodies.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
6.18 Reporting on issues identified by internal vulnerability scanning is reviewed by the Technology Leadership Team on a weekly basis.	Inquired of management to obtain an understanding of how reporting on issues identified by internal vulnerability scanning were reviewed by the Technology Leadership Team. Inspected vulnerability management procedures to determine whether policies were in place regarding reporting vulnerability issues to the Technology Leadership Team. Inspected documentation for a selection of weeks to determine whether issues identified by vulnerability scanning were reported to the Technology Leadership Team on a weekly basis.	No exceptions noted.
6.19 A coverage analysis is performed quarterly to identify gaps in vulnerability scanning coverage. Identified coverage gaps are resolved timely.	Inquired of management to obtain an understanding of how the quarterly coverage analysis is performed to identify vulnerability scanning gaps. Inspected Visa Key Controls, Policies & Procedures to determine whether policies were in place regarding the identification of gaps in vulnerability scanning coverage. Inspected the coverage analysis for a selection of quarters to determine whether a coverage analysis was performed quarterly to identify gaps in vulnerability scanning coverage and that gaps were resolved timely.	No exceptions noted.
6.20 Data Loss Prevention (DLP) tools are employed to detect and prevent unauthorized disclosure of sensitive data.	Inquired of management to obtain an understanding of the DLP tools in place and how they were used to prevent unauthorized disclosure of sensitive data and how Visa uses Symantec Vontu DLP and McAfee Data Loss Prevention Endpoint (DLPe) systems to monitor the disclosure of sensitive data. Inspected the Visa Vontu Gateway Data Loss Prevention and McAfee Data Loss Prevention Endpoint – DLPe policies and procedures documents to determine whether the documents included instructions and guidelines for accessing the DLP consoles as well as monitoring, investigating and resolving DLP incidents. Inspected screenshots of both DLP consoles and dashboards obtained through walkthrough to determine whether the DLP tools are in	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 6 – Logical Security *Controls provide reasonable assurance that logical access to production data files and platforms are restricted to authorized individuals and the security environment is monitored.*		
	place and actively monitoring the disclosure of sensitive data.	
6.21 Penetration tests are conducted at least annually for selected network devices and selected application servers and resulting issues are monitored by management.	Inquired of management to obtain an understanding of whether internal penetration tests were conducted at least annually for network devices and production servers and the resulting issues were monitored by management. Inspected Visa Key Controls, Policies & Procedures to determine whether policies were defined for penetration testing. Inspected tracking documentation for penetration testing to determine whether internal penetration tests were conducted at least annually and whether test results were tracked.	No exceptions noted.
6.22 Procedures exist to identify, report, and act upon system security breaches and other incidents.	Inquired of management to obtain an understanding of the procedures established around identification, reporting and handling of system security breaches and other incidents. Inspected the Incident Response Guide to determine whether the procedures in place to identify, report, and act upon incidents and security breaches adequately explain the correct response.	No exceptions noted.

Application Development and Change Management

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 7 – Application Development and Change Management *Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.*		
7.1 Formal software development life cycle (SDLC) procedures are in place to guide application development and maintenance activities.	Inquired of management to obtain an understanding of the formal software development life cycle (SDLC) procedures that are in place to guide application development and maintenance activities. Inspected the software development life cycle documentation to determine whether formal SDLC procedures were documented to guide application development and maintenance activities.	No exceptions noted.
7.2 A source code revision control system is used to manage source code to production systems. Access to the code revision control system is restricted to authorized personnel.	Inquired of management to obtain an understanding of the source code revision control system in place to manage source code. Observed the AccuRev application to determine whether production systems source code revisions are tracked in the tool. Inspected a system-generated list of all users with access to the code revision control system to determine whether administrative access was restricted to release engineers and that developers do not have such access.	No exceptions noted.
7.3 Change management policies and procedures have been established and documented for normal and emergency changes into the production environment.	Inspected change management policies and procedures to determine whether change management policies and procedures had been defined for normal and emergency changes, were current, available from Visa's Intranet, and reviewed and updated by management on a periodic basis.	No exceptions noted.
7.4 Changes (normal and emergency) to the production environment are documented, tested and approved in accordance with policies and procedures using an automated workflow.	Inquired of management to obtain an understanding of how changes to the production environment were documented and approved in accordance with policies and procedures. Inspected change management process documentation to determine whether procedures to document and approve changes to the production	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 7 – Application Development and Change Management *Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.*		
	environment were consistent with management's description. Inspected the Business Change Management (BMC) Remedy system (VIPER) configuration during walkthrough to determine whether the system had controls that enforce the following required fields and approvals, as stated in policies and procedures: ▪ All required fields must be completed before a change ticket can be submitted, including the population of an approval group and testing group. ▪ QA cannot approve a change unless test results field is completed. ▪ A change request cannot reach the implementation schedule unless sign-offs from each group (approval and testing) have been obtained. Inspected group members for a selection of automated workflow approval and testing groups within the VIPER system to determine whether workflow groups were restricted to authorized personnel. Inspected the annual group membership review for a selection of automated workflow approval and testing groups within the VIPER system to determine whether group membership reviews were conducted by management at least annually, that access was appropriate and corresponding group membership modifications were performed. Inspected a selected change to production to determine whether changes to the production environment were documented, tested, and approved prior to implementation.	
7.5 Adequate segregation of duties exists to ensure that changes require the approval of someone other than the requestor of the change.	Inquired of management to obtain an understanding of whether adequate segregation of duties were in place to ensure that changes require the approval of someone other than the requestor of the change. Inspected change management process documentation to determine whether the procedures to ensure that changes require the approval of someone other than the requestor of the change were consistent with management's description.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 7 – Application Development and Change Management *Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.*		
	Inspected the Business Change Management (BMC) Remedy system configuration during walkthrough to determine whether segregation of duties was enforced by the system to ensure that changes require the approval of someone other than the requestor of the change.	
7.6 Management has implemented file integrity monitoring tool(s) to monitor changes to critical systems.	Inquired of management to obtain an understanding of the process of file integrity monitoring of changes to critical systems. Observed the file integrity monitoring tools to determine whether file integrity tool(s) have been implemented to monitor changes to production systems. Inspected CyberSource Tripwire reports for a selection of weeks to determine whether file updates to production systems were monitored and reviewed weekly for appropriateness. Inspected management review of Authorize.Net production changes for a selection days to determine whether file updates to production servers were reviewed daily for appropriateness.	No exceptions noted.
7.7 Application development and testing environments are segregated from the production systems environment.	Inquired of management to obtain an understanding of how application development and testing environments are segregated from production systems environment. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether it requires logically and/or physically separated production and non-production environments. Inspected listings of production and non-production servers to determine the names and IP addresses of production and non-production servers to check against the network diagram. Inspected network diagrams to determine whether they illustrate the separation of the production and non-production environments.	No exceptions noted.

Network Security, Management and Maintenance

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 8 – Network Security, Management and Maintenance *Controls provide reasonable assurance that the network is properly secured, managed, and maintained.*		
8.1 Firewalls are in place at the network perimeter and logically separate trusted and un-trusted network zones. Firewall rules are reviewed at least annually.	Inquired of management to obtain an understanding of whether firewalls are in place at the network perimeter and logically separate trusted and un-trusted network zones. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether firewalls are required to logically separate trusted and un-trusted network zones. Inspected the network diagrams to determine whether firewalls are in place at the network perimeter and logically separate trusted and un-trusted network zones. Inspected the annual review of firewall rule sets to determine firewalls were in place at the network perimeter and logically separate trusted and un trusted network zones.	No exceptions noted.
8.2 Network and host-based intrusion detection tools are installed to detect unauthorized access to network devices and application servers. Security events are logged, monitored, and exceptions are resolved in a timely manner.	Inquired of management to obtain an understanding of how network and host-based intrusion detection tools are used to detect unauthorized access to network devices and application servers and the process in place to log, monitor, and resolve security events. Inspected screenshots from the McAfee IntruShield application to determine whether network and host-based intrusion detection tools were installed to detect unauthorized access to network devices and application servers. Refer to **Problem Management 5.4** on page **4-15** for tests of operating effectiveness related to the documentation, tracking and resolution of identified network security events.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 8 – Network Security, Management and Maintenance *Controls provide reasonable assurance that the network is properly secured, managed, and maintained.*		
8.3 User access reviews are conducted by management semi-annually to ensure that access to update firewall rule sets is appropriate. If access is inappropriate, access modifications are made.	Inquired of management to obtain an understanding of the process of semi-annual user validation of access to update firewall rule sets conducted by management and how access modifications are made. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether that firewalls must be reviewed every six months. Inspected evidence from the semi-annual user access review of firewall access to determine whether management reviewed access to ensure that access is restricted to current employees with valid business purpose and job responsibilities that warrant access, and that any inappropriate access identified during the review was removed timely.	No exceptions noted.
8.4 Network components are implemented in a redundant configuration.	Inquired of management to obtain an understanding of how network components are implemented in a redundant configuration. Inspected the Visa Inc. Key Controls, Objectives and Standards documentation to determine whether policies and procedures describing the implementation of network components in a redundant configuration have been defined and are current. Observed the Check-Point application, used for centralized network security and management, to determine whether network components are implemented in a redundant configuration. Inspected the Visa Global Network Backbone Diagram to determine whether network components are implemented in a redundant configuration.	No exceptions noted.
8.5 A capacity plan is in place and system capacity and transaction volume is reviewed by management.	Inquired of management to obtain an understanding of the capacity planning that is performed on annual basis and how system capacity and transaction volumes are monitored. Inspected the Visa Inc. Key Control Policies and Procedures to determine whether policies and procedures for computer resource capacity planning are documented. Inspected the annual capacity plan to determine whether the plan is in place and the system capacity and transaction volume is reviewed by management.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 8 – Network Security, Management and Maintenance *Controls provide reasonable assurance that the network is properly secured, managed, and maintained.*		
8.6 Network changes follow the standard change management process.	Inquired of management to obtain an understanding of how network changes follow the change management process. Inspected Visa Inc. Key Controls Policies & Procedures to determine whether network change policies and procedures have been defined and current. Refer to **Application Development and Change Management 7.4** on page **4-25** for test of effectiveness procedures related to network changes are documented, tested.	No exceptions noted.

Transactional Controls

Control Objectives, Related Controls, and Tests of Operating Effectiveness Provided by KPMG LLP

Control Description	Test Performed	Test Results
Control Objective No. 9 – Transactional Controls *Control activities provide reasonable assurance that transaction billings are processed completely and accurately.*		
9.1 Transaction fees are automatically calculated on a monthly basis based on transaction volume and established pricing.	Inquired of management to obtain an understanding of how transaction fees used for invoicing clients are computed based upon the number of transactions incurred and the established pricing. Recalculated the monthly transaction fees for a sample merchant for Enterprise and Small Business to determine whether the monthly transaction fees are accurately calculated automatically based on number of transactions incurred and the established pricing.	No exceptions noted.
9.2 Program changes to transaction fee calculation are documented, tested, and approved prior to migration to production.	Inquired of management to obtain an understanding of how program changes to transaction fee calculations are made. Inspected documentation for a selection of program changes to transaction fee calculations to determine whether the changes were documented, tested, and approved prior to migration to production.	No exceptions noted.
9.3 Access to update established pricing tables is restricted to authorized personnel.	Inquired of management to obtain an understanding of how access to update pricing is limited to authorized personnel. Inspected HR documentation and the user listings from the financial/billing systems to determine whether access to update pricing is restricted to authorized personnel, based on job responsibilities.	No exceptions noted.
9.4 Updates to established pricing tables are documented and approved.	Inquired of management to obtain an understanding of the process of making updates to established pricing tables. Inspected supporting documentation for a selection of updates to established pricing tables during the period to determine whether pricing updates were approved.	No exceptions noted.

Control Description	Test Performed	Test Results
Control Objective No. 9 – Transactional Controls *Control activities provide reasonable assurance that transaction billings are processed completely and accurately.*		
9.5 A monthly analytic review is performed on customer activities, billable transactions and quotes information. Significant variance from plan and forecast are investigated and resolved.	Inquired of management to obtain an understanding of how monthly reviews are performed to verify customer activity, billable transactions and quotes information and that items that do not appear reasonable are investigated and resolved. Inspected the management review evidence for a selection of months to determine whether a monthly review is performed to verify customer activity, billable transactions and quotes information and whether items that do not appear reasonable are investigated and resolved.	No exceptions noted.

Security Certification and Validation

In addition to the annual SSAE 16/ISAE 3402 Type II assessment, each year CyberSource undergoes a number of other assessments of internal controls and is compliant with the regulatory and industry mandates and best practice frameworks summarized below.

PCI-DSS: The Payment Card Industry Data Security Standard (PCI-DSS) is a set of technical and operational security requirements designed to protect cardholder data and applies to all organizations that store, process or transmit cardholder data. CyberSource, including Authorize.Net, complies with the requirements of the PCI-DSS. CyberSource and Authorize.Net are validated annually as Level 1 Service Providers by a Qualified Security Assessor (QSA).

The 12 PCI-DSS requirements are listed below:

- **Build and maintain a secure network and systems**
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect cardholder data**
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a vulnerability management program**
  - Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications
- **Implement strong access control measures**
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Identify and authenticate access to system components
  - Requirement 9: Restrict physical access to cardholder data
- **Regularly monitor and test networks**
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- **Maintain an information security policy**
  - Requirement 12: Maintain a policy that addresses information security for all personnel

For more information on CyberSource's compliance with these standards, please refer to the **Attachment A** (PCI-DSS Attestation of Compliance)

For more information about the PCI-DSS please visit:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Legal Compliance

CyberSource is not currently subject to direct regulation by any domestic or foreign governmental agency, but may be subject to laws and regulations applicable to businesses generally, publicly traded companies, export control laws, and laws or regulations directly applicable to eCommerce. However, due to the increasing usage of the Internet, it is possible that a number of laws and regulations may be applicable or may be adopted in the future with respect to conducting business over the Internet covering issues such as: taxes; user privacy; pricing; content; right to access personal data; data transfer; intellectual property; distribution; and characteristics and quality of products and services. Following is a brief summary of some laws and regulations that may apply to CyberSource. This summary is by no means intended to be an exhaustive list or discussion and is being provided for illustrative purposes only.

DPA see UK Data Protection Act of 1998

Fair and Accurate Credit Transactions Act of 2003 (FACTA or FACT) a.k.a. "Red Flag Rules": The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations requiring "financial institutions" and "creditors" with "covered accounts" as well as "business associates" and "covered entities" to develop and implement written identity theft prevention programs. CyberSource regularly reviews laws and developments to assess the applicability to Company and Company's compliance with such laws, as appropriate. To learn more about FACTA and the "Red Flag Rules" please visit: http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.

GLBA see Gramm-Leach-Bliley Act of November 1999 (GLBA or GLB)

Gramm-Leach-Bliley Act of November 1999 (GLBA or GLB) a.k.a. The Financial Modernization Act of 1999: GLBA includes provisions to protect consumers' personally identifying information that is held by "financial institutions," both traditional (e.g. banking, securities firms, etc.) and nontraditional (e.g. tax services, credit counseling, law firms, insurance companies, etc.). GLBA includes: the Financial Privacy Rule, Safeguards Rule and pre-texting provisions. CyberSource regularly reviews laws and developments to assess the applicability to Company and Company's compliance with such laws, as appropriate. To learn more about the GLBA you may wish to visit: http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

Health Information Technology for Economic and Clinical Health (HITECH) Act: Passed as part of American Recovery and Reinvestment Act of 2009 (ARRA), HITECH includes provisions to ensure that individuals' health information is secured to the extent possible to avoid unauthorized uses and disclosures, and that individuals are appropriately notified when incidents do occur. CyberSource regularly reviews laws and developments to assess the applicability to Company and Company's compliance with such laws, as appropriate. To learn more about HITECH you may wish to visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechblurb.html.

HIPAA see Kennedy-Kassebaum Health Insurance Portability and Accountability Act of 1996

HITECH see Health Information Technology for Economic and Clinical Health (HITECH) Act

Kennedy Kassebaum Health Insurance Portability and Accountability Act of 1996 (HIPAA): HIPAA provides federal protections for personal health information held by covered entities and establishes rights of patients with respect to such information. CyberSource regularly reviews laws and developments to assess the applicability to Company and Company's compliance with such laws, as appropriate. To learn more about HIPAA you may wish to visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

Sarbanes Oxley: The Sarbanes Oxley Act of 2002 (SOX) was enacted to enhance the accuracy and timeliness of public company financial disclosures. As of July 21, 2010 CyberSource Corporation, including all of its subsidiaries and affiliates, was acquired by Visa Inc. Accordingly, CyberSource, as a standalone entity, is not required to comply with SOX. However, CyberSource's controls will be assessed as part of Visa's SOX compliance initiatives. Visa common stock is publicly traded on the New York Stock Exchange NYSE under the symbol "V". Visa Inc's filings with the U.S. Securities and Exchange Commission (SEC) are publicly available on the SEC website at http://www.sec.gov/edgar/searchedgar/companysearch.html.

UK Data Protection Act of 1998 ("DPA"): The DPA establishes rights for those who have their data stored, and responsibilities for those who store, process, collect personal data, or control personal data. CyberSource regularly reviews laws and developments to assess the applicability to Company and Company's compliance with such laws, as appropriate. To learn more about the DPA you may wish to visit: http://ico.org.uk/for_organisations/data_protection.

Privacy Policy

CyberSource and its subsidiaries, including but not limited to Authorize.Net LLC, CyberSource Ltd., CyberSource NI Ltd., CYBS Singapore Pte. Ltd., CyberSource K.K. and CyberSource Payment Solutions Pty. Ltd. (collectively "CyberSource") maintains a comprehensive Privacy Policy. The Privacy Policy describes CyberSource's procedures for collection, use, and disclosure, correction and deletion of personally identifiable information. CyberSource regularly reviews applicable laws and developments to assess the Company's compliance with such laws, as appropriate. The most current version of the Privacy Policy can be found at: http://www.cybersource.com/privacy.php.

Global Business Continuity

Overview

As a leading payments technology company, with a global network that connects thousands of financial institutions with millions of merchants and cardholders every day, Visa understands the need for uninterrupted reliability. At Visa, resilience is a continuous process of assessing, planning, testing, training, and finding new ways to improve upon how we operate.

Visa's Global Business Continuity (GBC) program employs a "best-in-class" program that puts seamless continuity of operations at the forefront of everything we do. The GBC program supports Visa's brand promise to provide the reliability that our clients and cardholders expect.

Governance

The GBC program is managed and executed, on an annual cycle, by a team of knowledgeable and experienced staff with a single mission to ensure "business as usual" in unusual times. All Visa entities are required to comply with this centrally managed program.

Staff and resources are allocated to three disciplines within GBC:

- **Crisis Management** focuses on emergency response and the management of incidents that threaten life, property, Visa's brand reputation, operations, external clients, products/services, or any part of the payment system. This discipline ensures an ongoing process to command, control, and direct a coordinated and effective response to any incident. It also directs workforce recovery and crisis communications internally and to our clients.
- **Business Continuity Management** focuses on business process continuity and recovery. This discipline identifies critical and essential business processes, establishes options for recovery, and ensures viability of plans through documentation, training, and exercising.
- **IT Disaster Recovery** focuses on the recovery of systems and applications. This discipline assesses application and service criticality, and ensures that the necessary plans are in place for the enterprise to provide a pre-determined level of IT operations.

  The program follows a well-established cycle of assessment, planning, testing/exercising, and training that is defined in Visa's corporate policy, key controls, a multi-year strategy and execution plan, and procedural documents. The program's design is based on regulatory guidance and industry standards, including:

  - Federal Financial Institution Examination Council (FFIEC) Business Continuity Planning IT Examination Handbook – February 2015
  - International Organization for Standardization (ISO) 22301 Business Continuity Management (replaced BS25999)
  - ASIS International SPC.1-2009 – Organizational Resilience: Security, Preparedness, and Continuity Management Systems
  - National Fire Protection Association (NFPA) 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs

Activities across GBC are coordinated by management in support of the program strategy, execution of which is pre-planned, and follows documented procedures. The Policy and Program Executive Sponsor is the EVP of Technology. The Policy and Program Owner is the head of Global Information Security. The Program is executed by the Global Business Continuity leaders and staff. Visa's governing committees regularly review and approve this program's policy, annual performance and interim

progress. Specifically, oversight of the Program is provided by the Audit Risk Committee, the Corporate Risk Committee and the Operational Risk Sub-Committee.

Independent assurance of the Program is provided by internal and external auditors. Consultants are also brought in regularly to assess the program and provide recommendations to raise the program's level of maturity.

Business Impact Analysis / Application Impact Analysis

Based on a risk-based approach, the Global Business Continuity Program at Visa annually assesses all business processes and applications to determine their criticality to the enterprise and the services provided by the corporation. The result of the assessment is used to identify recovery time objectives (RTO), recovery point objectives (RPO), assign recovery priority, identify risks, determine planning requirements, and define strategies that meet recovery requirements and mitigate risks.

Table 1. Business Process and Application Tiered Recovery Requirements

	Tier Real Time (RT)	Tier 0	Tier 1	Tier 2	Tier 3	Tiers 4 & 5
RTO	≤ 2 Minutes	< 1 Hour	≤ 24 Hours	≤ 3 Days	≤ 7 Days	≥8 Days
Classification	Critical			Essential		Deferrable
Plans	Business Continuity and Technical Recovery Plans developed and exercised for each office location in which process or application must be recovered.					No Plans Required

Plan Development and Maintenance

Visa develops and maintains a collection of comprehensive plans, unified through a Crisis Management Framework, to address continuity and recovery needs of key operations. These plans are based on combination of risk assessments, impact analysis and key business priorities. Each plan is reviewed and updated annually.

- Business Continuity Plans (BCP) – location-based recovery plans for business processes identified as being critical or essential and with at least 6+ staff
- Technical Recovery Plans (TRP) – location-based recovery plans for applications and other technology identified as being critical or essential
- Data Center Recovery Plans (DCRP) – plans for recovering an entire data center after a catastrophic event
- Site Emergency Response Plans (SERP) – location-specific emergency plans for ensuring safety of staff and availability of facilities
- Global Incident Management Plan (GIMP) – an all-hazard plan that defines the framework for taking command and control of both life safety and business incidents
- Global Pandemic Plan – an action plan Visa will employ to prepare for and respond to the unique challenges posed by a pandemic. Based on World Health Organization (WHO) protocols, this plan encompasses all Visa Inc. locations and staff. The pandemic plan would be activated in conjunction with the GIMP and appropriate SERP.

- Business Incident Response Plans (BIRP) – specialized plans for managing a response to business incidents that would have a significant impact on Visa's critical business functions or brand/reputation, thereby hindering the ability to deliver key services to clients. For instance, individual plans cover incident scenarios that impact Visa's ability to move money via clearing and settlement or an outage/degradation to Visa core systems that impact our ability to authorize or process transactions. Additionally, BIRPs have been developed for incidents incurred by clients but are outside of Visa, such as an external data compromise, natural disaster, or technology disruption.
- Special Events Plans – short-term plans designed to deal with high-visibility, corporate-sponsored events, such as the Olympics, FIFA or the Super Bowl.

Plans are made available to recovery and incident management team members through the corporate Intranet, and other channels, to facilitate easy access. Repositories are replicated at multiple data centers.

Due to their confidential nature, plans are not available for review by third-parties.

Plan Exercising and Testing

Visa validates the efficacy of its plans annually at a minimum, to ensure the viability of plans and assurance of the continuity of operations as well as the readiness of plan participants. Exercise/test program requirements are evaluated at the beginning of the annual program cycle by the board and senior management for approval. Revisions to the requirements are based upon previous year's results, business needs/importance and independent party recommendations.

The testing methods and frequency of testing at Visa vary by plan and/or plan type. Activation (live production) tests are Visa's preferred form of exercise. In addition, scenario based functional-type exercises/tests are performed where Activation tests are not possible. Tabletop exercises are another form of exercise available, but restricted in use and used minimally given the limited value in demonstrating response and recovery capabilities.

Exercises are conducted using pre-established strategies, goals and evaluation criteria. Scenarios are changed and complexity is increased with each exercise/test, to highlight different types of risks and create new challenges for the recovery teams. Integrated exercises/tests – multiple plans associated with a core service, or multiple plans at a hub location or between business line and disaster recovery – are also performed where and when possible.

Technology with Active-Active infrastructure is regularly tested, through "failover", as part of standard operations. This failover is observed and documented by Global Business Continuity, as part of a scheduled activation exercise annually.

Exercise/Test results including action items and key learnings are documented, tracked and reported to several audiences including the board and senior/executive management at least annually. Results and key learnings are also incorporated into plan revisions.

Crisis Management Activation

Each crisis varies in type, criticality, magnitude, location, impacted parties, and other factors. Visa's Crisis Management Framework considers each of these differences in formulating a response.

It classifies incidents by type (Life Safety or Business), and then by severity level (minor, moderate or severe). The type and severity establishes the plan to be executed and the team to be activated.

Following a well-established protocol, the incident management team meets with regularity to assess the situation, review triggers and the need for escalation/de-escalation, and then develops and documents activities related to: people, facilities, technology, mission critical processes, clients, and communications. Timeframes for delivering on action items and next steps are defined and resources are assigned.

Training

Training is handled through various means for differing audiences. Visa staff are provided with general training through online training, information session events, informative content on Visa's intranet website, and annual email/phone/text notification tests. This provides them with information on what to do, who to contact, when, and how.

Those who have a role in business or technical recovery, and/or crisis management plans are provided with specific training, throughout the assessment, planning and exercise cycle, on:

- Roles and Responsibilities
- Activation/Deactivation Process
- Recovery/Response Strategy and Tasks
- Crisis Management Framework
- Incident Action Planning
- Communication Tools, Templates and Protocols

Communications

GBC is responsible for the formal communication protocols used during a crisis. It uses an externally hosted alert system to notify staff and provide direction during a situation, or to notify a team(s) of an activation and the commencement of a meeting.

Following each meeting, GBC sends a communication to all members of relevant teams. These communications are approved by the Incident Commander and summarize what is known about the event, decisions made, actions taken and/or planned. A copy is sent to the Executive Committee for moderate, severe, or catastrophic incidents.

Employee and client communications also are identified, and they are executed by Corporate Communications. Delivery-channel options include corporate email, a mass notification system, and an informational call-in number for staff, Intranet, Extranet, and manual calling. Client communications are handled through Visa's Client Support Service's account managers.

In addition to these communication channels, Visa also uses satellite phones which are distributed to offices around the globe, to ensure internal communications with senior management and key staff.

Corporate Communications regularly monitors media channels, including social media, and responds when appropriate.

Communication templates have been pre-developed and approved to cover a number of different scenarios and various stakeholder communication needs.

Client Communications and Services

Client Service and Communications are key considerations in the Incident Action Planning process. Representatives from Client Services and Corporate Communications participate on incident management and response teams. Our goal is to provide the right information through the most effective delivery channels to assist clients as quickly as possible.

Client support staff are distributed around the world and use a well-practiced global event management process to quickly address client needs during an incident.

Customer Care Centers employ a workload-shift strategy, enabling them to automatically shift calls between multiple locations in the US and around the world, as appropriate. Constant service level monitoring allows shifting resource requirements to be addressed quickly.

Technical Operations

Visa maintains multiple geo-distant Operation Centers around the world. Computer hardware, software and telecommunication networks with sufficient capacity are maintained to support recovery of mission-critical services and processes in the event of a planned or unplanned outage. Technical resources are dispersed across multiple Operations Centers to adequately address a potential loss of personnel at the impacted site.

Locations of Visa Operations Centers were selected through a process that included a threat and risk assessment (e.g. natural disasters, etc.). These Operations Centers feature physical protection, environmental monitoring, redundant communication networks, predefined backup facilities and procedures to allow the backup Operations Center to recover all critical services in a timely fashion.

Visa has deployed several advanced recovery technologies – such as synchronous and asynchronous data replication, dedicated hardware and software, and network routing capabilities – to support its ability to rapidly recover critical applications in the event of an unplanned outage. Data replication occurs over high-speed telecommunications links that allow almost instantaneous updates to a geographically distant recovery facility. Application and system software at alternate recovery sites are constantly updated and synchronized to maintain readiness capabilities.

Tools

Visa uses a number of tools as part of its Global Business Continuity Program:

- An assessment, planning and reporting tool to ensure standardization, data integrity, and compliance reporting
- An externally-hosted automated notification system to deliver alerts to staff around the globe
- A toll-free phone message system that allow staff to obtain information on the status of their office
- Satellite phones for key staff around the globe as an alternative communication method when local communication services are unavailable
- Communication templates for a wide variety of incident scenarios have been created to streamline and standardize communications with staff and clients during an incident

Management of Third Parties

Vendors provide technology and business services that allow Visa to provide innovative solutions around the globe. Ensuring that their recovery capabilities align with our needs is important to delivering on our promise of reliability. Visa has an extensive Supplier Risk Management Program (SRMP) that uses subject matter experts from across the enterprise, to determine a vendor's criticality and ability to meet business and control requirements throughout the lifecycle of the relationship. To do this, the Supplier Risk Management Program:

- Assesses the criticality of vendor services based on Visa's level of dependency and the impact that it would have if that service were unavailable, compromised, or not meeting service expectations
- Reviews vendor recovery capabilities
- Identifies and tracks potential risks
- Works with the business relationship owner to develop and implement a plan for addressing these risks; which may include:
    - Developing an internal recovery strategy for loss of vendor

  - Requiring the vendor to improve their controls within a specific timeframe
  - Replacing the vendor
- Works with Sourcing to ensure that the appropriate requirements are stipulated in contracts

Vendors deemed as critical to Visa are required to undergo periodic on-site audits, performed by Information Security's Governance, Risk, & Compliance team. This audit looks at the controls in place around data security, business continuity, and PCI compliance. If the vendor is found to be out of compliance with Visa business and/or control requirements, the vendor is placed on a watch list, and remains there until their deficiencies have been successfully addressed, or until Visa terminates the relationship. Once on the watch list, Visa senior management must approve the plan for addressing the vendor risks.

Global Business Continuity also identifies vendor dependencies as part of the Business Impact Analysis and then develops strategies and tasks as part of the Business Continuity Plan to minimize the impact of a vendor failure.

Outsourced Technology

Visa is actively working on a phased approach to address all key elements outlined in Appendix J: Strengthening the Resiliency of Outsourced Technology Services ("Appendix J") within the recently released, February 2015, update to the FFIEC's Business Continuity Planning IT Examination Handbook.

Specifically, Visa is preparing to act in accordance with all four key elements outlined in the Appendix:

1. Third-Party Management
2. Third-Party Capacity
3. Testing with Third-Party Technology Service Provider (TSP)
4. Cyber Resilience

ATTACHMENT A (PAGE 1)

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

April 2015

ATTACHMENT A (PAGE 2)

PCI Security Standards Council

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	CyberSource Corporation		DBA (doing business as):	CyberSource, Authorize.Net , CyberSource KK, and CyberSource Managed Hosting	
Contact Name:	Christian Wagner		Title:	Director, Global Compliance	
ISA Name(s) (if applicable):	Not Applicable		Title:	Not Applicable	
Telephone:	(650) 432-8317		E-mail:	cwagner@visa.com	
Business Address:	900 Metro Center Blvd.		City:	Foster City	
State/Province:	CA	Country:	USA	Zip:	94404
URL:	http://www.visa.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Trustwave				
Lead QSA Contact Name:	Victor G. Smith		Title:	Security Consultant	
Telephone:	(312) 873-7500		E-mail:	vsmith@trustwave.com	
Business Address:	70 West Madison Street, Suite 1050		City:	Chicago	
State/Province:	IL	Country:	USA	Zip:	60602
URL:	http://www.trustwave.com				

ATTACHMENT A (PAGE 3)

PCI Security Standards Council

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	CyberSource US (including Authorize.net), CyberSource Managed Hosting, CyberSource KK	
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☒ Hardware ☒ Infrastructure / Network ☒ Physical space (co-location) ☒ Storage ☒ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☒ Fraud and Chargeback	☒ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☒ Billing Management	☐ Loyalty Programs	☐ Records Management
☒ Clearing and Settlement	☒ Merchant Services	☐ Tax/Government Payments
☒ Network Provider		
☐ Others (specify):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."*

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

ATTACHMENT A (PAGE 4)

PCI Security Standards Council

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *August 31, 2015*, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of *August 31, 2015*: (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *CyberSource Corporation* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

ATTACHMENT A (PAGE 5)

PCI Security Standards Council

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Qualys*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date:* 9/1/15
Service Provider Executive Officer Name: **Sunil Seshadri**	*Title:* **Chief Information Security Officer**

Part 3c. QSA Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	*Assessment of the environment and review of compliance with PCI DSS requirements outlined in PCI DSS v3.1.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: August 31, 2015*
Duly Authorized Officer Name: Victor G. Smith	*QSA Company:* Trustwave

Part 3d. ISA Acknowledgement (if applicable)	
If an ISA was involved or assisted with this assessment, describe the role performed:	*Not Applicable*

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

ATTACHMENT A (PAGE 6)

PCI Security Standards Council

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	