Payment Card Industry (PCI)

Card Production Security Assessors (CPSA) Logical and Physical

Qualification Requirements

Version 1.2
March 2024

Document Changes

Date	Version	Description
April 2019	1.0	Initial Release of the *Card Production Security Assessor Qualification Requirements – Logical and Physical Controls*
March 2022	1.1	▪ Added requirement for CPSAs to have appropriate skills for assessments ▪ Added requirement that CPSAs must be trained on the version of standard they are using ▪ Added requirement for periodic checks on QA process ▪ Added requirement that QA staff at CPSA Company is a CPSA or has CPSA Informational Training ▪ Removed requirements on the CPSA Legacy program ▪ Performed minor clarifications in language throughout
March 2024	1.2	▪ Added requirement for annual QA Questionnaire in section 6.2 ▪ Changed "Information Training" references to "Knowledge Training" throughout

Table of Contents

1 Introduction

These Card Production Security Assessor (CPSA) Qualification Requirements are intended for companies and their employees wishing to qualify under the PCI SSC CPSA Program and describe the minimum capability and related documentation requirements that a candidate CPSA Company or CPSA Employee must satisfy to be qualified by PCI SSC to perform any PCI Card Production Assessment.

- **The *PCI Card Production and Provisioning Logical Security Requirements*** ("PCI Card Production Logical Security Requirements") addresses the logical security controls associated with card production and provisioning such as:
  - EMV data preparation
  - Pre-personalization
  - Card embossing
  - IC and magnetic-stripe personalization
  - PIN generation
  - PIN mailers
  - Card carriers
  - Distribution
- **The *PCI Card Production and Provisioning Physical Security Requirements*** ("PCI Card Production Physical Security Requirements") addresses the physical security controls associated with card production activities such as:
  - Card Manufacturing
  - Chip embedding
  - Personalization
  - Storage
  - Mailing
  - Shipping or delivery
  - Fulfillment

This document outlines the requirements for qualification as a CPSA Company or CPSA Employee.

The PCI Card Production Logical Security Requirements and PCI Card Production Physical Security Requirements are maintained by PCI SSC and available through the Website.

1.1 Terminology

Throughout these CPSA Qualification Requirements, the following terms shall have the following meanings:

Term	Meaning
Assessor Portal (Portal)	Web-based application made available to PCI SSC-qualified assessors to access PCI SSC program documentation and forms.
Card Production Entity	A company that performs card production and provisioning activities such as card manufacturing, chip imbedding, data preparation, pre-personalization, card embossing, integrated chip (IC) and magnetic-stripe personalization, PIN generation, PIN mailers, card carriers, and distribution.
Card Production Security Assessor (CPSA) Company	A company that has been qualified, and continues to be qualified, by PCI SSC to perform PCI Card Production Assessments.
Card Production Security Assessor (CPSA) Employee	An employee of a CPSA Company who has been qualified, and continues to be qualified, by PCI SSC to perform PCI Card Production Assessments.
Card Production Security Assessor – Logical Controls (CPSA-L)	A CPSA Employee who satisfies and continues to satisfy all CPSA Requirements for qualification by PCI SSC to perform Logical PCI Card Production Assessments.
Card Production Security Assessor – Physical Controls (CPSA-P)	A CPSA Employee who satisfies and continues to satisfy all CPSA Requirements for qualification by PCI SSC to perform Physical PCI Card Production Assessments.
Card Production Security Assessor (CPSA) List	The then-current list of CPSA Assessor Companies published by PCI SSC on the Website.
Card Production Security Assessor (CPSA) Program	The program operated by PCI SSC in connection with which companies and their employees may achieve qualification by PCI SSC for purposes of performing assessments of compliance with the PCI Card Production Logical Security Requirements and/or the PCI Card Production Physical Security Requirements for purposes of such program, as further described herein and in the CPSA Program Guide.
Card Production Security Assessor (CPSA) Program Guide	The then-current version of the *PCI Card Production Security Assessor Program Guide*, as from time to time amended and made available on the Website. The CPSA Program Guide provides guidance to primary contacts and assessors on the CPSA Program.

Term	Meaning
CPSA Agreement	The then-current version of the CPSA Company Agreement attached as Appendix A to the CPSA Qualification Requirements.
CPSA Annual QA Questionnaire	The then-current version of the CPSA Annual QA Questionnaire form available on the Portal.
CPSA Requirements	With respect to a given CPSA Company or CPSA Employee, the applicable requirements and obligations thereof pursuant to the CPSA Qualification Requirements, the CPSA Program Guide, the CPSA Agreement, each addendum, supplement, or other agreement or attestation entered into between such CPSA Company or CPSA Employee and PCI SSC, and any and all other policies, procedures, requirements, validation or qualification requirements, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time in connection with the CPSA Program, including but not limited to all policies, procedures, requirements, standards, obligations of all applicable training programs, quality-assurance programs, remediation programs, program guides, and other related CPSA Program materials, including without limitation those relating to probation, fines, penalties, oversight, remediation, suspension and/or revocation.
Card Production Security Requirements	The set of security requirements as documented in the then-current *Payment Card Industry (PCI) Card Production and Provisioning Logical Security Requirements* and *Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements.*
Logical PCI Card Production Assessment	Assessment of a Card Production Entity to validate compliance with the PCI Card Production Logical Security Requirements for CPSA Program purposes.
PCI Card Production Assessment	Logical PCI Card Production Assessment or Physical PCI Card Production Assessment.
PCI Card Production Security Requirements	The then-current versions of (or successor documents to) the *PCI Card Production Logical Security Requirements* and the *PCI Card Production Physical Security Requirements,* as from time to time amended and made available on the Website.
Physical PCI Card Production Assessment	Assessment of a Card Production Entity to validate compliance with the PCI Card Production Physical Security Requirements for CPSA Program purposes.
Template for Card Production Report on Compliance (Card Production ROC)	The mandatory template for documenting and reporting the results of a PCI Card Production Assessment to Participating Payment Brands, as made available on the Website.
Website	The then-current PCI SSC Web site (and its accompanying Web pages), which is currently available at http://www.pcisecuritystandards.org.

All capitalized terms used in these CPSA Qualification Requirements without definition shall have the meanings ascribed to them in the CPSA Agreement, as applicable.

1.2 Qualification Process Overview

The CPSA Program qualification process involves the qualification of the company and each candidate CPSA Employee thereof who will be performing PCI Card Production Assessments.

To initiate the qualification process, the candidate CPSA Company must sign the CPSA Agreement (Appendix A) in unmodified form and submit it to PCI SSC along with the company's executed CPSA Company Application (See Appendix C). Additionally, a CPSA Employee Application (See Appendix D for CPSA – Logical Controls, Appendix E for CPSA – Physical Controls) must be completed for each company employee seeking CPSA Employee qualification and submitted to PCI SSC.

1.3 Document Structure

This document (among other things) defines the requirements that CPSA Companies and CPSA Employees must meet to become Card Production Security Assessors. The document is structured in four sections as follows:

Section 1: Introduction offers a high-level overview of the CPSA Program application process.

Section 2: CPSA Company Business Requirements covers minimum business requirements that must be met by the CPSA Company prior to joining the CPSA Program. This section outlines everything the CPSA Company must provide to PCI SSC.

Section 3: CPSA Program Capability Requirements reviews the information and documentation necessary to demonstrate the CPSA Company's service expertise, as well as the qualifications of its employees.

Section 4: CPSA Company Administrative Requirements focuses on the standards to meet regarding the logistics of doing business as a CPSA Company, including adherence to PCI SSC procedures documented in the CPSA Program Guide, quality assurance, and protection of confidential and sensitive information.

1.4 Related Publications

This document should be used in conjunction with the current, publicly available version of the following other PCI SSC publications (or successor documents), each available through the PCI SSC Website:

- *Payment Card Industry (PCI) Card Production and Provisioning Logical Security Requirements*
- *Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements*
- *Payment Card Industry (PCI) Card Production Security Assessors (CPSA) Program Guide*

1.5 Card Production Security Assessor Application Process

This document describes the information that must be provided to PCI SSC as part of the CPSA application and qualification process. Each outlined requirement is followed by the information that must be submitted to document that the CPSA Company and CPSA Employee meet or exceed the stated requirements.

All company applications must include a signed CPSA Agreement (Appendix A) and a completed and signed application form for each candidate CPSA Employee (in accordance with Section 3.2.2 below), which can be found in Appendices D and E. The CPSA Agreement is binding in English even if the CPSA Agreement was translated and reviewed in another language. All other documentation provided by the CPSA Company (or candidate) in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

Applicants should submit their completed application packages to PCI SSC via the Assessor Portal.

Applications that have not been approved or rejected after 180 days from submittal will be deleted.

Important Note: *PCI SSC reserves the right to reject any application from any applicant (company or employee) that PCI SSC determines has committed, within three (3) years prior to the application date, any conduct that would have been considered a "Violation" for purposes of the CPSA Qualification Requirements or CPSA Agreement if committed by a CPSA Company or CPSA Employee. The period of ineligibility will be a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner, in light of the circumstances.*

1.6 Additional Information Requests

In an effort to maintain the integrity of the CPSA Program, PCI SSC may request from time to time that CPSA Companies and/or CPSA Employees submit additional information or materials in order to demonstrate adherence to applicable requirements, as part of the applicable qualification or requalification process, or as part of the CPSA Program approval or quality-assurance process, including but not limited to in connection with remediation, revocation, or appeals. All such information and materials must be submitted in accordance with the corresponding PCI SSC request, in English or with a certified English translation, within three (3) weeks of the corresponding PCI SSC request, or as otherwise requested by PCI SSC.

2 CPSA Company Business Requirements

This section describes the minimum business requirements for CPSA Companies, and related information that must be provided to PCI SSC by each candidate CPSA Company regarding its business legitimacy, independence, and required insurance coverage.

2.1 Business Legitimacy

2.1.1 Requirement

Each candidate CPSA Company must be recognized as a legal entity.

2.1.2 Provisions

The following information must be provided to PCI SSC:

- Copy of current CPSA Company (or candidate CPSA Company) formation document or equivalent approved by PCI SSC (the "Business License"), including year of incorporation and list of location(s) of offices (Refer to PCI Business License Requirements in the Documents Library on the Website for more information.)
- To the extent permitted by applicable law, written statements describing all past or present allegations or convictions of any fraudulent or criminal activity involving the CPSA Company, CPSA Company candidate or any principal thereof, and any CPSA Employee or CPSA Company candidate thereof, and the status and resolution.
- Written statements describing any past or present appeals or revocations of any qualification issued by PCI SSC to the CPSA Company (or any predecessor entity or, unless prohibited by applicable law, any CPSA Employee of any of the foregoing), and the current status and any resolution thereof.

2.2 Independence

2.2.1 Requirement

The CPSA Company must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI Card Production Assessments.

The CPSA Company must have a code-of-conduct policy and provide the policy to PCI SSC upon request. The CPSA Company's code-of-conduct policy must support—and never contradict—the PCI SSC Code of Professional Responsibility.

The CPSA Company must adhere to all independence requirements as established by PCI SSC, including without limitation, the following:

- The CPSA Company will not undertake to perform any PCI Card Production Assessment of any entity that it controls, is controlled by, is under common control with, or in which it holds any investment.

Note: *CPSA Employees are permitted to be employed by only one CPSA Company at any given time*.

- The CPSA Company must not (and will not) have offered, been offered, been provided, or have accepted any gift, gratuity, service, or other inducement to any employee of PCI SSC or to any customer, in order to enter into the CPSA Agreement or any agreement with a customer, or to provide CPSA Company-related services.
- The CPSA Company must fully disclose in the Card Production ROC if it assesses any customer that uses any security-related device, application, product, or solution that is developed, manufactured, sold, resold, licensed, or otherwise made available to the applicable customer by the CPSA Company, or to which the CPSA Company owns the rights, or that the CPSA Company has configured or manages, including but not limited to the following:
  - Application or network firewalls
  - Intrusion detection/prevention systems
  - Database or other storage solutions
  - Encryption solutions
  - Security audit log solutions
  - File integrity monitoring solutions
  - Anti-virus solutions
  - Vulnerability scanning services or solutions
  - EMV Data Preparation Solutions
  - Personalization Equipment
- The CPSA Company must not recommend products or solutions for remediating findings but can make Card Production Entities aware of solutions that exist.
- The CPSA Company must enforce separation of duties to ensure CPSA Employees conducting PCI Card Production Assessments are not subject to any conflict of interest.
- The CPSA Company will not use its status as a “listed CPSA Company” to market services unnecessary to bring CPSA Company clients into compliance with the PCI Card Production.
- The CPSA Company must not misrepresent any requirement of the PCI Card Production Security Requirements in connection with its promotion or sales of services to its clients, or state or imply that the PCI Card Production Security Requirements require usage of the CPSA Company's products or services.
- The CPSA Company must notify its CPSA Employees of the independence requirements provided for in this document, as well as CPSA Company’s independence policy, at least annually.

2.2.2 Provisions

The CPSA Company (or candidate CPSA Company) must describe its practices to maintain and assure employee and CPSA Company independence with respect to all PCI Card Production Assessments, including but not limited to practices, organizational structure, separation of duties, and employee education in place to prevent conflicts of interest. The description must address each requirement listed in Section 2.2.1.

2.3 Insurance Coverage

2.3.1 Requirement

At all times while its CPSA Agreement is in effect, the CPSA Company shall maintain such insurance coverage, exclusions, and deductibles with such insurers as PCI SSC may reasonably request or require to adequately insure the CPSA Company for its obligations and liabilities under the CPSA Agreement, including without limitation the CPSA Company's indemnification obligations.

The CPSA Company must adhere to all requirements for insurance coverage required by PCI SSC, including without limitation the requirements in Appendix B, “Insurance Coverage,” which includes details of required insurance coverage.

2.3.2 Provisions

The CPSA Company (or candidate CPSA Company) must provide a proof-of-coverage statement to PCI SSC to demonstrate that insurance coverage matches PCI SSC requirements and locally set insurance coverage requirements (see Appendix B).

2.4 CPSA Company Fees

2.4.1 Requirement

Each CPSA Company must provide to PCI SSC all fees required by PCI SSC in connection with the CPSA Company’s (or its CPSA Employees’) participation in the CPSA Program (collectively, “CPSA Program Fees”).

- CPSA Company fees
- Annual CPSA Company requalification fees for subsequent years
- Annual training fee for each CPSA Employee (or candidate)

Note: *All CPSA Program fees are specified on the Website in the PCI SSC Programs Fee Schedule and are subject to change.*

2.5 CPSA Agreements

2.5.1 Requirement

In order to participate in the CPSA Program, PCI SSC requires that all agreements between PCI SSC and the CPSA Company (including the CPSA Agreement) be signed by a duly authorized officer of the CPSA Company and submitted in unmodified form to PCI SSC prior to submitting applicants to the CPSA Program. Pursuant to the CPSA Agreement, the CPSA Company agrees to comply with all applicable CPSA Requirements.

3 CPSA Program Capability Requirements

This section describes the minimum capability requirements for CPSA Companies and CPSA Employees, as well as the related documentation that all CPSA Companies and CPSA Employees must provide to PCI SSC in order to demonstrate requisite technical security audit expertise, work history, and industry experience.

3.1 CPSA Company – Services and Experience

3.1.1 Requirements

The CPSA Company must possess technical security assessment experience similar or related to PCI Card Production Assessments.

The CPSA Company must have a dedicated information security practice that includes staff with specific job functions that support the information security practice.

A CPSA Company must have at least one CPSA Employee at all times.

3.1.2 Provisions

The following information must be provided to PCI SSC:

- Description of the applicant CPSA Company's experience and knowledge with information security audit engagements, preferably related to payment systems, equal to at least one year or three separate audits
- Description of the applicant CPSA Company's relevant areas of specialization within information security—for example, network security, database and application security, and incident response—demonstrating at least one area of specialization
- Evidence of a dedicated security practice, such as:
  - The total number of employees on staff and the number of those performing security assessments
- Brief description of other core business offerings
- List of languages supported by the applicant CPSA Company
- Two client references from security engagements performed by the applicant CPSA Company within the last 12 months

3.2 CPSA Employee – Skills and Experience

Each CPSA Employee performing or managing PCI Card Production Assessments must be qualified by PCI SSC as either a Card Production Security Assessor – Logical Controls, or a Card Production Security Assessor – Physical Controls. While in good standing or in remediation, a Card Production Security Assessor – Logical Controls is qualified by PCI SSC to conduct assessments against the PCI Card Production Logical Security Requirements, and a Card Production Security Assessor – Physical Controls is qualified by PCI SSC to conduct assessment against the PCI Card Production Physical Security Requirements. A CPSA Employee may qualify for either or both categories. CPSA Employees (for both Logical Controls and Physical Controls) are responsible for the following:

- Performing Logical or Physical (as applicable) PCI Card Production Assessments.
- Verifying the work product addresses all PCI Card Production Assessment procedure steps and supports the validation status of the Card Production Entity.
- Strictly following the PCI Card Production and Provisioning Security Requirements (both Logical and Physical).
- Producing the final Card Production Report on Compliance (ROC) and Card Production Attestation of Compliance (AOC).

3.2.1 Requirements

3.2.1.1 CPSA Employee for Logical Controls Status Requirements

Each CPSA Employee performing or managing Logical PCI Card Production Assessments must satisfy the following requirements:

- Pass background checks required per Section 4.2.
- Possess a minimum of five years of experience in Cryptography and/or Key Management which includes:
  - Cryptographic techniques including cryptographic algorithms, key management, and key lifecycle
  - Knowledge of industry standards for cryptographic techniques and key management, including but not limited to ISO 11568 and 13491, ANSI X9.24 and X9.97, and FIPS 140-2
  - Public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA)
  - Hardware security modules (HSMs) operations, policies, and procedures
  - Physical security techniques for high-security areas
  - Key-loading devices (KLDs) and key-management methods, such as Master/Session or DUKPT
- Possess a minimum of five years of experience in network security and systems security. A working knowledge of application security is highly recommended.
- Possess at least five years of experience in IT auditing or security assessments.

- Possess at least one of the following accredited, industry-recognized professional certifications from each list:
  - **List A – Information Security**
    - (ISC)2 Certified Information System Security Professional (CISSP)
    - ISACA Certified Information Security Manager (CISM)
    - Certified ISO 27001 Lead Implementer1
  - **List B – Audit**
    - ISACA Certified Information Systems Auditor (CISA)
    - GIAC Systems and Network Auditor (GSNA)
    - Certified ISO 27001, Lead Auditor, Internal Auditor [1]
    - IRCA ISMS Auditor or higher e.g., Auditor/Lead Auditor, Principal Auditor
    - IIA Certified Internal Auditor (CIA)

Note: *"Provisional" auditor designations do not meet the requirement.*

- Be an employee of the CPSA Company.

3.2.1.2 CPSA Employee for Physical Controls Status Requirements

Each CPSA Employee performing or managing Physical PCI Card Production Assessments must satisfy the following requirements:

- Pass background checks required per Section 4.2.
- Possess a minimum of four years of work experience in physical security or have a current Physical Security Professional (PSP) or Certified Protection Professional (CPP) certification with two years of work experience in physical security.
- Possess a minimum of four years of experience in physical security audits or have a current certification from List B (see 3.2.1.1 above) with three years of experience in physical security audits.

[1] ISO27001 certifications will be accepted as meeting the requirement only when certifications are issued by an accredited certification body—for example, ANSI-ASQ National Accreditation Board (ANAB) and United Kingdom Accreditation Service (UKAS). Certified ISO 27001 courses should be accredited to the ISO/IEC 17024 standard. It is the responsibility of the company/candidate to ensure that the certifying body is accredited, and to provide evidence of accreditation to PCI SSC.

To find out whether your country has an accreditation body, visit the International Accreditation Forum (IAF) website at www.iaf.nu and use the IAF MLA signatories list to identify an accreditation body in your country or region.

To find a certification body, visit the International Organization for Standardization certification information page; the section titled "Choosing a certification body" will explain how to find a certification body.

Verification of company's certification should be addressed to the certification organization in question. You may also wish to contact the ISO member in your country or the country concerned, as it may have a national database of certified companies.

- Possess a minimum of three years of experience in system security. System security refers to the logical security of systems that provide or enforce physical security—e.g., CCTV and access-control systems.
- Be an employee of the CPSA Company.

3.2.1.3 CPSA Employee Training Requirements

Prior to performing any PCI Card Production Assessment and annually thereafter, the CPSA Employee must successfully complete and pass annual CPSA Program training and training examinations required by PCI SSC. Individuals who fail any such exam are not permitted to lead or manage any PCI Card Production Assessment until passing the exam on a future attempt. CPSA Employees are only authorized to perform PCI Card Production Assessments using major versions of the Card Production Security Requirements for which they have successfully completed the corresponding CPSA Program training and training examination.

3.2.2 Provisions

The following information must be provided to PCI SSC for each candidate CPSA Employee:

- Record of years of relevant work experience and active certifications as outlined in 3.2.1 above.
- Résumé or Curriculum Vitae (CV) of each candidate CPSA Employee.
- Completion and submission of Appendix D for each candidate CPSA Employee – Logical Controls and Appendix E for each candidate CPSA Employee – Physical Controls.

3.3 PCI SSC Code of Professional Responsibility

3.3.1 Requirement

PCI SSC has adopted the PCI SSC Code of Professional Responsibility (the "Code") to help ensure that CPSA Companies and CPSA Employees adhere to high standards of ethical and professional conduct. All CPSA Companies and CPSA Employees must advocate, adhere to, and support the Code (available on the Website).

4 CPSA Company Administrative Requirements

This section describes the administrative requirements for CPSA Companies, including company contacts, background checks, adherence to PCI CPSA procedures, quality assurance, and protection of confidential and sensitive information.

4.1 Contact Person

4.1.1 Requirements

The CPSA Company must provide PCI SSC with a primary and secondary contact. If the CPSA Company is already a PCI Qualified Security Assessor (QSA) Company in good standing, it may indicate the same contacts to be used on the form in Appendix C.

4.1.2 Provisions

The following contact information must be provided to PCI SSC, for both primary and secondary contacts (see Appendix C):

- Name
- Job title
- Address
- Phone number
- Fax number
- E-mail address

4.2 Background Checks

4.2.1 Requirements

Each CPSA Company must perform background checks that satisfy the provisions described below (to the extent legally permitted within the applicable jurisdiction) with respect to each applicant CPSA Employee.

Minor offenses—for example, misdemeanors or non-US equivalents—are allowed; but major offenses—for example, felonies or non-US equivalents—automatically disqualify a candidate from qualifying as an CPSA Employee. Upon request, each CPSA Company must provide to PCI SSC the background check history for each CPSA Employee (or candidate CPSA Employee), to the extent legally permitted within the applicable jurisdiction.

Note: *PCI SSC reserves the right to decline or reject any application or applicant CPSA Employee.*

4.2.2 Provisions

The CPSA Company (or candidate CPSA Company) must provide PCI SSC with responses to each of the following (see Appendix C):

- Attestation that its policies and hiring procedures include performing background checks: Examples of background checks include previous employment history, criminal record, credit history, and reference checks.

- A written statement that it successfully completed such background checks for each candidate CPSA Employee.
- A summary description of current CPSA employee personnel background check policies and procedures, which must require and include the following:
  - Verification of aliases (when applicable)
  - Comprehensive country and (if applicable) state level review of records of any criminal activity such as felony (or non-US equivalent) convictions or outstanding warrants, within the past five years minimum
  - Annual background checks consistent with this section for each of its CPSA Employees for any change in criminal records, arrests or convictions

4.3 Internal Quality Assurance

4.3.1 Requirements

- The CPSA Company must adhere to all CPSA Program quality-assurance requirements described in this document or otherwise established by PCI SSC from time to time.
- The CPSA Company must have a quality-assurance (QA) program, documented in its Quality Assurance manual.
- The CPSA Company must maintain and adhere to a documented quality-assurance process and manual, which includes all of the following:
  - Company name
  - A resource planning policy and process for PCI Card Production Assessments which includes: onboarding requirements for CPSA Employees, résumés and current skill sets for CPSA Employees, and a process for ongoing training, monitoring, and evaluation of CPSA Employees to ensure their skill sets stay current and relevant for PCI Card Production Security Assessments
  - Descriptions of all job functions and responsibilities within the CPSA Company relating to its status and obligations as a CPSA Company
  - Identification of QA manual process owner
  - Approval and sign-off processes for PCI Card Production Assessments and respective reports
  - Requirements for independent quality review of CPSA Company and CPSA work product
  - Requirements for internal periodic checks, at least annually, of the CPSA Company's QA program to monitor the effectiveness and evolving QA processes of such QA program
  - Requirements for handling and retention of workpapers and other Assessment Results and Related Materials (defined in the CPSA Agreement; see also Section 4.5 for specific requirements for Workpaper Retention Policy requirements and specifications)

- QA process flow
- Distribution and availability of the QA manual
- Evidence of annual review by the QA manual process owner
- Coverage of all quality-assurance activities relevant to the CPSA Program, and references to the CPSA Qualification Requirements
- Requirement for all CPSA Employees to regularly monitor the Website for updates, guidance, and new publications relating to the CPSA Program

- The CPSA Company must have qualified personnel (independent of the assessing and/or authoring CPSA Employee) conduct a quality-assurance review of assessment procedures performed, supporting documentation workpapers retained in accordance with CPSA Company's Workpaper Retention Policy, information documented in the Card Production ROC related to the appropriate selection of system components, sampling procedures, remediation recommendations, proper use of payment definitions, consistent findings, and thorough documentation of results.
- All quality-assurance reviews must be conducted by personnel that are either CPSA Employees or other personnel that have completed CPSA Knowledge Training. CPSA Knowledge Training must be completed initially and after every major update in the Card Production Security Requirements prior to reviewing submissions under the new release.
- The CPSA Company should require all new CPSA Employees, who have not previously performed a PCI Card Production assessment or a Card Production Entity assessment under a Legacy Program to shadow a CPSA Employee on at least one (1) PCI Card Production Assessment prior to conducting an assessment by themselves.
- The CPSA Company must inform each PCI Card Production Assessment client of the CPSA Feedback Form (available on the Website) upon commencement of each PCI Card Production Assessment.
- PCI SSC, at its sole discretion, reserves the right to conduct audits of the CPSA Company at any time and further reserves the right to conduct site visits at the expense of the CPSA Company.
- Upon request by PCI SSC, the CPSA Company must annually complete the CPSA Annual QA Questionnaire in the Portal for PCI SSC quality monitoring purposes.
- Upon request, the CPSA Company (or applicant) must provide a complete copy of the quality-assurance manual to PCI SSC.

4.3.2 Provisions

The applicant CPSA Company must provide completed Appendix C to PCI SSC.

4.4 Protection of Confidential and Sensitive Information

4.4.1 Requirement

- The CPSA Company must have and adhere to a documented process for protection of confidential and sensitive information. This must include adequate physical, electronic, and

procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.

- The CPSA Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties and obligations as a CPSA Company, unless (and to the extent) disclosure is required by legal authority.

4.4.2 Provisions

The CPSA Company (or applicant) must attest that its documented process for protection of confidential and sensitive information includes the following (see Appendix C):

- Physical, electronic, and procedural safeguards including:
  - Protection of systems storing customer data by network and application layer controls including technologies such as firewall(s) and IDS/IPS
  - Restricting access—e.g., via locks—to the physical office space
  - Restricting access—e.g., via locked file cabinets—to paper files
  - Restricting logical access to electronic files via least-privilege/role-based access control
  - Strong encryption of customer data when transmitted over public networks
  - Secure transport and storage of backup media
  - Strong encryption of customer data on portable devices such as laptops and removable media

The CPSA Company must provide to PCI SSC a blank copy of the CPSA Company's confidentiality agreement(s) that each CPSA Employee is required to sign.

4.5 Evidence (Assessment Workpaper) Retention

4.5.1 Requirement

- Assessment Results and Related Materials (defined in the CPSA Agreement), including but not limited to PCI Card Production Assessment workpapers and related materials, represent the evidence generated and/or gathered by a CPSA Company to support the contents of each Card Production ROC or assessment report. Retention of Assessment Results and Related Materials is required and the Assessment Results and Related Materials relating to a given PCI Card Production Assessment should represent all steps of the PCI Card Production Assessment from end-to-end. Such Assessment Results and Related Materials may include screen captures, config files, interview notes, and a variety of other materials and information (and typically will include all of the foregoing). The CPSA Company must maintain and adhere to a documented retention policy regarding all Assessment Results and Related Materials (a "Workpaper Retention Policy"), which includes, minimally, the following: Formal assignment of an employee responsible for ensuring the continued accuracy of the Workpaper Retention Policy and that each CPSA Employee (a) complies with the Workpaper Retention Policy and (b) signs an appropriate confidentiality agreement with the CPSA Company (as contemplated by Section 4.4 above).

- A blank copy of the CPSA Company's Workpaper Retention Policy agreement that each CPSA Employee is required to sign, included as part of the policy, which includes agreement to conform at all times with the Workpaper Retention Policy and the CPSA Qualification Requirements.
- A requirement that all Assessment Results and Related Materials must be classified as confidential and handled accordingly, with detailed instructions describing how CPSA Employees are to comply with this requirement. If the classification and handling of confidential information is addressed in other confidential and sensitive data protection handling policies of the CPSA Company, this should be clearly noted within the Workpaper Retention Policy.
- A requirement that Assessment Results and Related Materials must be retained for at least three (3) years and must include all digital and hard copy evidence created and/or obtained by or on behalf of the CPSA Company during each PCI Card Production Assessment—including but not limited to: documentation reviewed (policies, processes, procedures, network and dataflow diagrams), case logs, meeting agendas and notes, evidence of onsite and offsite activities (including interview notes), screenshots, config files, results of any tests performed, and any other relevant information created and/or obtained.
- Requirements ensuring that the CPSA Company has confirmed that all Assessment Results and Related Materials relating to a given PCI Card Production Assessment have been retained in accordance with the procedures defined in the Workpaper Retention Policy, prior to releasing the final Card Production ROC or assessment report for that PCI Card Production Assessment.
- All Assessment Results and Related Materials must be made available to PCI SSC and/or its Affiliates upon request for a minimum of three (3) years after completion of the applicable PCI Card Production Assessment.
- The CPSA Company must provide a copy of the Workpaper Retention Policy and related procedures to PCI SSC upon request, including copies of any other policies and procedures referenced within any of the foregoing documents, such as general confidential and sensitive data protection handling policies for the CPSA Company.

4.5.2 Provisions

- The applicant CPSA Company must provide completed Appendix C to PCI SSC.

4.6 Security Incident Response

This section describes obligations for CPSA Companies where breach of cardholder data in a customer's environment has or is suspected to have occurred.

4.6.1 Requirement

The CPSA Company must have and adhere to a documented process for notifying the applicable customer when the CPSA Company or any employee, contractor, or other personnel thereof, during or in connection with the performance of any PCI Card Production Assessment or other CPSA Program-related services, becomes aware of an actual or suspected breach of cardholder data within that customer's environment (each an "Incident"). Such process must require, and provide instruction for, notifying the customer in writing of the Incident and related findings, and

informing the customer of its obligations to notify the Participating Payment Brands in accordance with each Participating Payment Brands' notification requirements.

The customer notification must be documented and retained in accordance with the CPSA Company's evidence-retention policy, along with a summary of the Incident and what actions were taken in connection with the Incident and corresponding discovery and/or notification. CPSA Companies and CPSA Employees are required to be familiar with the obligations for reporting Incidents to each of the Participating Payment Brands.

If a PFI Investigation (see the *PCI Forensic Investigator (PFI) Program Guide* on the Website for additional details) is required by a Participating Payment Brand, a CPSA Company or CPSA Employee shall take no action after an Incident that is reasonably likely to diminish the integrity of, otherwise interfere with, or negatively affect the ability of a PCI Forensic Investigator to perform such PFI Investigation.

Failure to provide such written notification to the customer or otherwise comply with any of the above (or any other) CPSA Qualification Requirements constitutes a "Violation" (see Section 6.3 below) and may result in remediation, revocation, and/or termination of the CPSA Agreement.

4.6.2 Provisions

The applicant CPSA Company must attest (see Appendix C) that it has an internal Incident-response plan, including but not limited to:

- Instructions and procedures for notifying customers of Incidents discovered during or in connection with the performance of any PCI Card Production Assessment or other CPSA Program-related services and documenting those Incidents and related information in accordance with Section 4.6.1.
- Retention requirement for all incident-related documentation, notices, and reports, with the same protections as those noted for work-paper retention in the CPSA Company's evidence-retention policy and procedures.

5 CPSA List and Annual Requalification

This section describes what happens after initial qualification and activities related to annual requalification.

5.1 CPSA List

Once a company has met applicable CPSA Qualification Requirements and has at least one qualified CPSA Employee, PCI SSC will add the CPSA Company to the CPSA List on the Website.

Once an individual has met applicable CPSA Requirements, PCI SSC will add the CPSA Employee to the applicable CPSA Employee listing on the Website.

Only those CPSA Companies and CPSA Employees on the CPSA List are recognized by PCI SSC to perform or support PCI Card Production Assessments

Each CPSA Company must ensure that each of its CPSA Employees only works on those PCI SSC program assessments for which the CPSA Employee is properly qualified by PCI SSC, having appropriate skills, including technology and language, and having an appropriate understanding of the client's business.

If, at any time, a CPSA Company and/or CPSA Employee does not meet the applicable CPSA Requirements (including without limitation, payment or documentation requirements), PCI SSC reserves the right to immediately remove the CPSA Company and/or CPSA Employee from the respective list(s) on the Website, regardless of Remediation or Revocation. PCI SSC will notify the CPSA Company of the removal in accordance with the CPSA Agreement, typically via registered or overnight mail and/or e-mail. Refer to Sections 6.2 and 6.3 below for additional information relating to Remediation and Revocation.

5.2 Annual Requalification

5.2.1 Requirements

All CPSA Companies must be requalified by PCI SSC on an annual basis. The annual requalification date is based upon the CPSA Company's *original qualification date*. Requalification requires payment of annual training and requalification fees, and continued compliance with applicable CPSA Requirements.

A CPSA Employee must requalify on an annual basis by their requalification date for each CPSA program with which they have certification. In order to requalify:

CPSA-L must:

(a) Complete at least three (3) Logical PCI Card Production Assessments for different facilities over the previous one-year period ***and*** complete PCI SSC computer-based CPSA Logical training course/exam

or

(b) Successfully complete PCI SSC instructor-led CPSA Logical training course and exam.

CPSA-P must:

(a) Complete at least three (3) Physical PCI Card Production Assessments for different facilities over the previous one-year period ***and*** complete PCI SSC computer-based CPSA Physical training course/exam

or

(b) Successfully complete PCI SSC instructor-led CPSA Physical training course and exam.

The annual requalification date is based upon the CPSA Employee's *previous qualification date*. Requalification requires proof of training successfully completed, payment of annual training and requalification fees, and continued compliance with applicable CPSA Requirements.

Negative feedback from CPSA Company clients, PCI SSC, Participating Payment Brands, or others may impact CPSA Company and/or CPSA Employee eligibility for requalification.

5.2.2 Provisions

The following must be provided to PCI SSC during each annual requalification process:

- **CPSA Companies**
  - Payment of annual CPSA Company fees
- **CPSA Employees**
  - Proof that the CPSA Employee has completed at least three PCI Card Production Assessments for different facilities over the last one-year period, for each CPSA Program Certification **and** completion of required PCI computer-based CPSA training and exam ***OR*** has attended CPSA Instructor-led Logical and/or Physical training over the last one-year period.

    ***Note*:** *CPSA Employees that do not complete the required number of assessments must register and complete the PCI SSC CPSA Instructor-led training and exam prior to their requalification date to remain listed as an active assessor. PCI SSC CPSA Instructor-led training is subject to availability.*
  - CPSA-P Employees without professional certifications must provide proof of Continuing Professional Education within the last 12 months in accordance with the current version of the *PCI SSC CPE Maintenance Guide*.
  - Maintaining professional certification(s) as required per Section 3.2, "CPSA Employee – Skills and Experience." PCI SSC reserves the right to request proof of current professional certifications at any time.
  - Payment of annual requalification fees in accordance with the Website – PCI SSC Programs Fee Schedule.

Note: *PCI SSC may from time to time request that CPSA Companies and/or CPSA Employees submit additional information or materials in order to demonstrate adherence to applicable requirements or as part of the applicable qualification or requalification process.*

6 Assessor Quality Management Program

The PCI SSC's Assessor Quality Management (AQM) team exists to monitor and review assessor work in order to provide reasonable assurance that assessors maintain a baseline standard of quality. In addition to the audit process, the AQM team receives feedback on CPSA Companies from the Participating Payment Brands using a scorecard. Refer to the CPSA Program Guide, Appendix B, "Eight Guiding Principles Validated by Four Criteria," on the website to understand PCI SSC's baseline for assessor quality.

6.1 CPSA Audit Process

PCI SSC reserves the right to audit a CPSA Company at any time, and further reserves the right to conduct site visits at the expense of the CPSA Company.

6.2 CPSA Annual QA Questionnaire Process

CPSA Companies must annually complete the CPSA Annual QA Questionnaire for quality monitoring purposes, upon request by PCI SSC. The CPSA Company will be notified of PCI SSC's request for the CPSA Company to complete the CPSA Annual QA Questionnaire via the Portal. The notification will specify the information and materials the CPSA Company must provide as part of the CPSA Annual QA Questionnaire, which may include but is not limited to internal QA manuals, documented processes such as the Workpaper Retention Policy, Card Production ROC excerpts redacted in accordance with PCI SSC policy and other data specified in the notice.

The AQM team will review the completed CPSA Annual QA Questionnaire to monitor the CPSA Company's on-going adherence to program requirements and provide relevant feedback in the Portal.

6.3 CPSA Quality Remediation Process

CPSA Companies that do not meet all applicable quality-assurance standards set by PCI SSC for the CPSA Program may be offered the option to participate in PCI SSC's CPSA Company Quality Remediation program ("Remediation"). Without limiting the generality of the foregoing, PCI SSC may offer Remediation in connection with any quality-assurance audit, any Violation (defined below), or any other CPSA Program-related quality concerns, including but not limited to unsatisfactory feedback from CPSA Company customers or Participating Payment Brands. When a CPSA Company qualifies for Remediation, the CPSA Company will be notified in accordance with the CPSA Agreement, typically via registered or overnight mail and/or e-mail. Once the CPSA Company signs the agreement to participate in Remediation ("Remediation Agreement") and pays the fee(s) required in the notification, the applicable listing on the CPSA List will be annotated with "In Remediation" and the listing will display the CPSA Company's details in red text. Refer to the Website – *PCI SSC Programs Fee Schedule* for details of all applicable fees.

At the time of notification that the CPSA Company qualifies for Remediation, AQM will provide the CPSA Company with information on the requirements and procedures of the Remediation process and what it entails. Once AQM has gained sufficient assurance of quality improvement and confirmed to the CPSA Company in writing that the requirements of the Remediation Agreement have been fulfilled, Remediation ends, and the CPSA Company's listing on the Website returns to "In Good Standing" in black text. CPSA Companies that fail to satisfy Remediation requirements may be revoked, and CPSA Companies electing not to participate in Remediation when eligible will be revoked.

Note: *The* Remediation Statement *on the Website affirms the Council's position on Remediation, and any external queries about a CPSA Company's status will be directed to the CPSA Company in question.*

CPSA Companies in remediation may continue to perform PCI Card Production Assessments for which they are qualified by PCI SSC unless otherwise instructed by PCI SSC in connection with the Remediation process.

6.4 CPSA Revocation Process

Each event below is an example of a "Violation" (defined in the CPSA Agreement) and accordingly, regardless of prior warning or Remediation, may result in revocation of CPSA Company and/or CPSA Employee qualification. This list is not exhaustive.

- Failure to meet applicable CPSA Program quality standards or comply with applicable CPSA Requirements
- Failure to pay applicable CPSA Program fees
- Failure to meet applicable CPSA Program training requirements (annual or otherwise)
- Failure to provide quality services, based on customer feedback or evaluation by PCI SSC or its affiliates
- Failure to maintain applicable CPSA Program insurance requirements
- Failure to timely submit the CPSA Annual QA Questionnaire to PCI SSC in the Portal
- Failure to comply with or validate compliance in accordance with applicable CPSA Requirements, PCI Card Production Security Requirements or program guides, or the terms of the CPSA Agreement.
- Failure to maintain physical, electronic, or procedural safeguards to protect confidential or sensitive information
- Failure to report unauthorized access to any system storing confidential or sensitive information
- Engaging in unprofessional or unethical business conduct, including without limitation, plagiarism or other improper use of third-party work product in Card Production ROCs.
- Failure to comply with any provision or obligation regarding non-disclosure or use of confidential information or materials
- Cheating on any exam in connection with CPSA Program training; submitting exam work in connection with CPSA Program training that is not the work of the individual candidate taking the exam; theft of or unauthorized access to CPSA Program exam content; use of an alternate, stand-in or proxy during any CPSA Program exam; use of any prohibited or unauthorized materials, notes, or computer programs during any such exam; or providing or communicating in any way any unauthorized information to another person, device, or other resource during any CPSA Program exam
- Providing false or intentionally incomplete or misleading information to the Council in any application or other materials
- Failure to be in Good Standing (as defined in the CPSA Agreement) as a CPSA Company or CPSA Employee, including but not limited to failure to successfully complete applicable quality-assurance audits and/or comply with all applicable requirements, policies, and procedures of

PCI SSC's quality-assurance, remediation, and oversight programs and initiatives as established or imposed from time to time by PCI SSC in its sole discretion

- Failure to promptly notify PCI SSC of any event described above that occurred within three (3) years of the CPSA Company's or CPSA Employee's initial qualification date

Each Violation constitutes a breach of the CPSA Agreement and a failure to comply with applicable CPSA Requirements, and may result in revocation of CPSA Company and/or CPSA Employee qualification.

If the decision is made to revoke any CPSA Program qualification, notification will be provided in accordance with the CPSA Agreement and will include information regarding the appeal process.

Appeals must be submitted within 30 days from the date of the notification to the CPSA Program Manager by postal mail to the following address (e-mail submissions will not be accepted):

PCI SSC
401 Edgewater Place, Suite 600
Wakefield, MA 01880, USA

In connection with revocation, the following will occur:

- The CPSA Company and/or CPSA Employee (as applicable) name will be removed from the CPSA List and/or search tool (as applicable).
- PCI SSC may notify third parties.
- A company and/or individual (as applicable) the Qualification of which has been revoked can reapply after 180 days; provided however, that (i) if revoked in connection with Remediation, an election not to participate in Remediation when offered, or due to failure to satisfy applicable quality-assurance standards set by PCI SSC, such company and/or individual shall be ineligible to re-apply to the CPSA Program for a period of two (2) years; and (ii) acceptance of qualification applications after revocation is determined at the Council's discretion in a reasonable and nondiscriminatory manner, in light of the relevant facts and circumstances, including but not limited to the nature and severity of the violation, occurrence of repeat violations, and the applicant's demonstrated ability to comply with remediation requirements (if applicable).

Appendix A: CPSA Company Agreement

A.1 Introduction

This document (the "Agreement") is an agreement between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned Applicant ("CPSA"), regarding CPSA's qualification and designation to perform the Services (as defined in this document). PCI SSC and CPSA are each sometimes referred in this document as a "party" and collectively as the "parties." Effective upon the date of PCI SSC's approval of this Agreement (the "Effective Date"), as evidenced by the PCI SSC signature below, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, CPSA and PCI SSC agree to the terms and conditions set forth in this Agreement.

A.2 General Information

Applicant					
Company Name:					
Business Address:			City:		
State/Province:		Country:		ZIP/Postal Code:	
Regions					
Language(s) to be displayed on Listing:					

Primary Contact			
Name:		Job Title:	
Direct Telephone Number:		E-mail:	
Location:		Fax:	

Secondary Contact			
Name:		Job Title:	
Direct Telephone Number:		E-mail:	
Location:		Fax:	

Applicant CPSA Company Officer			
Applicant Officer Name:		Job Title:	
Applicant's Officer Signature ↑		*Date* ↑	

PCI SSC		
Name:		
Job Title:		
PCI SSC Signature ↑	*Date* ↑	

A.3 Terms and Conditions

A.3.1 CPSA Services

Subject to the terms and conditions of this Agreement, while CPSA is in Good Standing (defined in Section A.5.1(a) below) as a CPSA Company or in compliance with Remediation, PCI SSC hereby approves CPSA to perform, in accordance with this Agreement and the CPSA Qualification Requirements (defined below), reviews of Card Production Entities (each herein referred to as a "CPSA Company client"), to determine CPSA Company clients' compliance with the PCI Card Production Security Requirements as part of the CPSA Program. For purposes of this Agreement: (i) the reviews described above that are conducted by CPSA are referred to herein as "PCI Card Production Assessments"; (ii) the PCI Card Production Assessments, collectively with all related services provided by CPSA to PCI SSC, CPSA Company clients or others in connection with this Agreement and the CPSA Program, are referred to herein as the "Services"; (iii) "CPSA Qualification Requirements" means the most current version of (or successor document to) the *Payment Card Industry (PCI) Qualification Requirements for Card Production Security Assessors (CPSA)* document as available through the Website, as may be amended from time to time in PCI SSC's discretion, including without limitation, any and all additional supplements or addenda thereto which are applicable to CPSA as a result of its participation in the CPSA Program and related Card Production Security Assessor initiatives operated by PCI SSC (each of which initiatives is hereby deemed to be included within the meaning of the term "CPSA Program" for purposes of this Agreement); (iv) "Member" means an entity, as of the time in question, that is then formally admitted as (or an affiliate of) a member of PCI SSC in accordance with its governing documents (status as a PCI SSC "Participating Organization" does not establish that an entity is a "Member"); (v) "Participating Payment Brand" means a payment card brand that, as of the time in question, is a Member or affiliate thereof; (vi) "Qualification" means a qualification granted by PCI SSC under the CPSA Program; and (vii) unless otherwise indicated, all capitalized terms used in this Agreement without definition shall have the meanings ascribed to them in the CPSA Qualification Requirements. The CPSA Qualification Requirements are hereby incorporated into this Agreement, and CPSA acknowledges and agrees that it has reviewed the current version of the CPSA Qualification Requirements available on the Website.

CPSA acknowledges that data security practices exist within a rapidly changing environment and agrees to monitor the Website at least weekly for changes to the PCI Card Production Security Requirements and the CPSA Qualification Requirements. CPSA will incorporate all such changes into all applicable PCI Card Production Assessments initiated on or after the effective date of such changes. CPSA acknowledges and agrees that any Card Production ROC or other required report regarding a PCI Card Production Assessment that is not conducted in accordance with the PCI Card Production Security Requirement as in effect at the initiation date of such PCI Card Production Assessment may be rejected.

A.3.2 Performance of Services

CPSA Company warrants, represents, and agrees that it will only perform PCI Card Production Assessments for which it has been and is then qualified by PCI SSC, and that it will perform each such PCI Card Production Assessment in strict compliance with the applicable PCI Card Production Security Requirement(s) as in effect as of the commencement date of such PCI Card Production Assessment. Without limiting the foregoing, CPSA will include in each Card

Production ROC, a Card Production Attestation of Compliance (in the form available through the Website signed by a duly authorized officer of the CPSA , in which the CPSA certifies without qualification that (a) in performing such PCI Card Production Assessment, the CPSA Employee followed the requirements and procedures of the PCI Card Production Security Requirements without deviation and (b) application of such requirements and procedures did not indicate any conditions of non-compliance with the applicable PCI Card Production Security Requirements other than those expressly noted in the applicable Card Production ROC.

A.3.3 CPSA Service Staffing

CPSA shall ensure that a CPSA Employee that is fully qualified in accordance with all applicable *CPSA Requirements* supervises all aspects of each engagement to perform Services, including without limitation, being present onsite for the duration of each PCI Card Production Assessment (or monitoring remotely in accordance with the *PCI SSC Remote Assessment Guidelines and Procedures*), reviewing the work product that supports CPSA's PCI Card Production Assessment procedures, and ensuring adherence to the CPSA Qualification Requirements. Employees performing the following tasks must also be qualified as CPSA Employees: scoping decisions, selection of systems and system components where sampling is employed (in accordance with the PCI Card Production Security Requirements), evaluation final report production, and/or review. CPSA hereby designates the individual identified as the “Primary Contact” in Section A.2 above as CPSA’s primary point of contact and “Primary Contact” for purposes of the CPSA Program and this Agreement. The CPSA may change its Primary Contact at any time upon written notice to PCI SSC, and hereby represents that each Primary Contact shall have authority to execute any and all decisions on CPSA’s behalf concerning CPSA Program matters.

A.3.4 CPSA Requirements

CPSA agrees to comply with all CPSA Requirements, including without limitation, CPSA’s responsibilities and obligations pursuant to this Agreement, all CPSA Program quality-assurance and Remediation requirements, and all requirements applicable to CPSA pursuant to the CPSA Qualification Requirements. Without limiting the foregoing, CPSA agrees to comply with all requirements of, make all provisions provided for in, and ensure that its CPSA Employees comply with all applicable CPSA Qualification Requirements, agrees to comply with all such requirements regarding background checks, and warrants that it has obtained all required consents to such background checks from each employee designated by CPSA to PCI SSC to perform Services hereunder. CPSA warrants that, to the best of CPSA's ability to determine, all information provided to PCI SSC in connection with this Agreement and CPSA's participation in the CPSA Program is and shall be accurate and complete as of the date such information is provided. In the event of any change as a result of which any such information is no longer accurate or complete (including but not limited to any change in CPSA’s circumstances or compliance with applicable CPSA Requirements), CPSA shall promptly (and in any event within thirty (30) days after such change) notify PCI SSC of such change and provide such information as may be necessary to ensure that the information PCI SSC has received is then accurate and complete. CPSA acknowledges that PCI SSC from time to time may require CPSA to provide a representative and/or CPSA Employees to attend any mandatory training programs in connection with the CPSA Program, which may require the payment of attendance and other fees by CPSA.

A.4 Fees

CPSA agrees to pay all applicable fees imposed by PCI SSC in connection with CPSA's and its employees' participation in the CPSA Program (collectively, "Fees"), in each case as and in the manner provided for in the CPSA Qualification Requirements, the *PCI SSC Programs Fee Schedule* on the Website and/or the other applicable CPSA Program documentation. Such Fees may include, without limitation, company fee, training fees, fees in connection with quality assurance and/or remediation, penalties and other costs, and other fees. CPSA agrees to pay all such Fees as and when required by PCI SSC and that all Fees are nonrefundable (regardless of whether CPSA's application is approved, CPSA has been removed from the CPSA List, this Agreement has been terminated, or otherwise).

CPSA acknowledges that PCI SSC may review and modify its Fees at any time and from time to time. Whenever a change in Fees occurs, PCI SSC shall notify CPSA in accordance with the terms of Section A.10.1. Such change(s) will be effective immediately after the date of such notification. However, should CPSA not agree with such change(s), CPSA shall have the right to terminate this Agreement upon written notice to PCI SSC in accordance with the provisions of Section A.10.1 at any time within 30 days after such notification from PCI SSC. Except to the extent otherwise expressly provided in the CPSA Qualification Requirements or other applicable CPSA Program documentation, all fees payable to PCI SSC in connection with the CPSA Program must be paid in US dollars (USD), by check, by credit card, or by wire transfer to a PCI SSC bank account specified for such purpose by PCI SSC. CPSA acknowledges and agrees that such Fees do not include any taxes, such as value added taxes (VAT), sales, excise, gross receipts and withholding taxes, universal service fund fee, or any similar tax or other government-imposed fees or surcharges which may be applicable thereto. CPSA shall pay all such taxes and fees as invoiced in accordance with local law, and agrees to pay or reimburse PCI SSC for all such taxes or fees, excluding tax on PCI SSC's income. In respect of withholding tax, CPSA will pay such additional amounts as may be necessary, such that PCI SSC receives the amount it would have received had no withholding been imposed.

A.5 Advertising and Promotion; Intellectual Property

A.5.1 CPSA List and CPSA Use of PCI Materials and Marks

(a) So long as CPSA is qualified by PCI SSC as a CPSA Company, PCI SSC may, at its sole discretion, display the identification of CPSA, together with related information regarding CPSA's status as a CPSA Company (including without limitation, good standing, remediation and/or revocation status), in such publicly available lists of CPSA Companies as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (collectively, the "CPSA List"). CPSA shall provide all requested information necessary to ensure to PCI SSC's satisfaction that the identification and information relating to CPSA on the CPSA List is accurate. Without limiting the rights of PCI SSC set forth in the first sentence of this Section or elsewhere, PCI SSC expressly reserves the right to remove CPSA from the CPSA List at any time during which CPSA is not in Good Standing as a CPSA Company. CPSA shall be deemed to be in "Good Standing" with respect to the CPSA Program as long as this Agreement is in full force and effect, CPSA has been approved as a CPSA Company and such approval has not been revoked, CPSA is not in breach of any of the terms or conditions of this Agreement (including without limitation, any term or provision regarding compliance with the CPSA Qualification Requirements or payment).

(b) In advertising or promoting its Services, so long as CPSA is in Good Standing as a CPSA Company, CPSA may make reference to the fact that CPSA is listed in the CPSA List, provided that it may do so only during such times as CPSA actually appears in the CPSA List.

(c) Except as expressly authorized herein, CPSA shall not use any PCI SSC trademark, service mark, certification mark, logo, or other indicator of origin or source (each a “Mark”) without the prior written consent of PCI SSC in each instance. Without limitation of the foregoing, absent the prior written consent of PCI SSC in each instance and except as otherwise expressly authorized herein, CPSA shall have no authority to make, and consequently shall not make, any statement that would constitute any implied or express endorsement, recommendation, or warranty by PCI SSC regarding CPSA, any of its services or products, or the functionality, quality, or performance of any aspect of any of the foregoing. CPSA shall not: (i) make any false, misleading, incomplete, or disparaging statements or remarks regarding, or misrepresent the requirements of, PCI SSC or the PCI Card Production Security Requirements, including without limitation, any requirement regarding the implementation of the PCI Card Production Security Requirements or the application thereof to any third party, or (ii) state or imply that the PCI Card Production Security Requirements require usage of CPSA's products or services. Subject to the foregoing, and except with respect to (A) factual references that CPSA includes from time to time in its contracts with CPSA Company clients that are required or appropriate in order for CPSA to accurately describe the nature of the Services CPSA will provide pursuant to such contracts, and (B) references permitted pursuant to Section A.5.1(b) above, CPSA shall not, without the separate prior written agreement or consent of PCI SSC in each instance: (1) copy, create derivative works of, publish, disseminate, or otherwise use or make available the PCI Card Production Security Requirements, PCI Materials (defined in Section A.7.3). PCI SSC mark or any copy of, or statement or material (in any form) that incorporates any of the foregoing or any portion thereof or (2) incorporate any of the foregoing, the name of PCI SSC or the term “PCI SSC” into any product or service (in any form). Prior review and/or approval of such statements,

materials, or products by PCI SSC does not relieve CPSA of any responsibility for the accuracy and completeness of such statements, materials, or products or for CPSA's compliance with this Agreement or any applicable law. Except as otherwise expressly agreed by PCI SSC in writing, any dissemination or use of promotional or other materials or publicity in violation of Section A.5 shall be deemed a material breach of this Agreement and upon any such violation, PCI SSC may remove CPSA's name from the CPSA List and/or terminate this Agreement in its sole discretion.

A.5.2 Uses of CPSA Name and Designated Marks

CPSA grants PCI SSC and each Participating Payment Brand the right to use CPSA's name and trademarks, as designated in writing by CPSA, to list CPSA on the CPSA List and to include reference to CPSA in publications to Card Production Entities and the public regarding the CPSA Program. Neither PCI SSC nor any Participating Payment Brand shall be required to include any such reference in any materials or publicity regarding the CPSA Program. CPSA warrants and represents that it has authority to grant to PCI SSC and its Participating Payment Brands the right to use its name and designated marks as contemplated by this Agreement.

A.5.3 No Other Rights Granted

Except as expressly stated in this Section A.5, no rights to use any party's or Member's marks or other Intellectual Property Rights (as defined below) are granted herein, and each party respectively reserves all of its rights therein. Without limitation of the foregoing, except as expressly provided in this Agreement, no rights are granted to CPSA with respect to any Intellectual Property Rights in the PCI Card Production Security Requirements or any other PCI Materials.

A.5.4 Intellectual Property Rights

(a) All Intellectual Property Rights, title and interest in and the CPSA Program, the PCI Card Production Security Requirements and all other PCI Materials, all materials CPSA receives from PCI SSC, and each portion, future version, revision, extension, and improvement of any of the foregoing, are and at all times shall remain solely and exclusively the property of PCI SSC or its licensors, as applicable. Subject to the foregoing and to the restrictions set forth in Section A.6, so long as CPSA is in Good Standing as a CPSA Company or in compliance with Remediation, CPSA may, on a non-exclusive, non-transferable, worldwide, revocable basis, use the PCI Materials (and any portion thereof), provided that such use is solely for CPSA's internal review purposes or as otherwise expressly permitted in this Agreement or pursuant and subject to the terms of a separate written consent or agreement between PCI SSC and CPSA in each instance. For purposes of this Agreement, "Intellectual Property Rights" shall mean all present and future patents, trademarks, service marks, design rights, database rights (whether registrable or unregistrable, and whether registered or not), applications for any of the foregoing, copyright, know-how, trade secrets, and all other industrial or intellectual property rights or obligations whether registrable or unregistrable and whether registered or not in any country.

(b) All right, title and interest in and to the Intellectual Property Rights in all materials generated by or on behalf of PCI SSC with respect to CPSA are and at all times shall remain the property of PCI SSC. Subject to the provisions of Section A.6, CPSA may use and disclose such materials solely for the purposes expressly permitted by this Agreement. CPSA shall not revise, abridge, modify, or alter any such materials.

(c) CPSA shall not during or at any time after the completion, expiry, or termination of this Agreement in any way question or dispute PCI SSC's or its licensors' (as applicable) Intellectual Property Rights in the CPSA Program or any of the PCI Materials.

(d) Except as otherwise expressly agreed by the parties, as between PCI SSC and CPSA, all Intellectual Property Rights, title and interest in and to the materials created by CPSA and submitted by CPSA to PCI SSC in connection with its performance under this Agreement are and at all times shall remain vested in CPSA, or its licensors.

A.6 Confidentiality

A.6.1 Definition of Confidential Information

As used in this Agreement, "Confidential Information" means (i) all terms of this Agreement; (ii) any and all information designated in this Agreement as Confidential Information; (iii) any and all originals or copies of, any information that either party has identified in writing as confidential at the time of disclosure; and (iv) any and all Personal Information, proprietary information, merchant information, technical information or data, assessment reports, trade secrets or know-how, information concerning either party's past, current, or planned products, services, fees, finances, member institutions, acquirers, issuers, concepts, methodologies, research, experiments, inventions, processes, formulas, designs, drawings, business activities, markets, plans, customers, equipment, card plastics or plates, software, source code, hardware configurations, or other information disclosed by either party or any Member, or their respective directors, officers, employees, agents, representatives, independent contractors, or attorneys, in each case, in connection with any CPSA Program or activity in which CPSA is a participant and in whatever form embodied—e.g., oral, written, electronic, on tape or disk, or by drawings or inspection of parts or equipment or otherwise—including without limitation, any and all other information that reasonably should be understood to be confidential. "Personal Information" means any and all Participating Payment Brand payment card account numbers, Participating Payment Brand transaction information, IP addresses or other PCI SSC, Member, or third-party information relating to a natural person, where the natural person could be identified from such information. Without limiting the foregoing, Personal Information further includes any information related to any Participating Payment Brand accountholder that is associated with or organized or retrievable by an identifier unique to that accountholder, including accountholder names, addresses, or account numbers.

A.6.2 General Restrictions

(a) Each party (the "Receiving Party") agrees that all Confidential Information received from the other party (the "Disclosing Party") shall: (i) be treated as confidential; (ii) be disclosed only to those Members, officers, employees, legal advisers, accountants, representatives, and agents of the Receiving Party who have a need to know and be used solely as required in connection with (A) the performance of this Agreement and/or (B) the operation of such party's or its Members' respective payment card data security compliance programs (if applicable) and (iii) not be disclosed to any third party except as expressly permitted in this Agreement or in writing by the Disclosing Party, and only if such third party is bound by confidentiality obligations applicable to such Confidential Information that are in form and substance similar to the provisions of this Section A.6.

(b) Except with regard to Personal Information, such confidentiality obligation shall not apply to information which: (i) is in the public domain or is publicly available or becomes publicly available otherwise than through a breach of this Agreement; (ii) has been lawfully obtained by the Receiving Party from a third party; (iii) is known to the Receiving Party prior to disclosure by the Disclosing Party without confidentiality restriction; or (iv) is independently developed by a member of the Receiving Party's staff to whom no Confidential Information was disclosed or communicated. If the Receiving Party is required to disclose Confidential Information of the Disclosing Party in order to comply with any applicable law, regulation, court order, or other legal, regulatory, or administrative requirement, the Receiving Party shall promptly notify the Disclosing Party of the requirement for such disclosure and co-operate through all reasonable and legal means, at the Disclosing Party's expense, in any attempts by the Disclosing Party to prevent or otherwise restrict disclosure of such information.

A.6.3 CPSA Company Client Data

To the extent any data or other information obtained by CPSA relating to any CPSA Company client in the course of providing Services thereto may be subject to any confidentiality restrictions between CPSA and such CPSA Company client, CPSA shall provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such CPSA Company client in writing) that (i) CPSA may disclose each Card Production ROC, Attestation of Compliance and other related or similar reports or information generated or gathered by CPSA in connection with its performance of the Services to PCI SSC and/or Participating Payment Brands, as requested by the CPSA Company client, (ii) to the extent any Participating Payment Brand obtains such reports or information in accordance with the preceding clause A6.3(i), such Participating Payment Brand may disclose (a) such reports or information on an as needed basis to other Participating Payment Brands and to such Participating Payment Brands' respective financial institutions and issuers and to relevant governmental, regulatory, and law enforcement inspectors, regulators, and agencies and (b) that such Participating Payment Brand has received a Card Production ROC, report and other related information with respect to such CPSA Company client (identified by name) and whether the Card Production ROC or report was satisfactory, and (iii) CPSA may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A.10.2(b) below. Accordingly, notwithstanding anything to the contrary in Section A.6.2(a) above, to the extent requested by a CPSA Company client, PCI SSC may disclose Confidential Information relating to such CPSA Company client and obtained by PCI SSC in connection with this Agreement to Participating Payment Brands in accordance with this Section A.6.3, and such Participating Payment Brands may in turn disclose such information to their respective member financial

institutions and other Participating Payment Brands. CPSA hereby consents to such disclosure by PCI SSC and its Participating Payment Brands. As between any Member, on the one hand, and CPSA or any CPSA Company client, on the other hand, the confidentiality of Card Production ROCs and any other information provided to Members by CPSA or any CPSA Company client is outside the scope of this Agreement and may be subject to such confidentiality arrangements as may be established from time to time between such Member, on the one hand, and CPSA or such CPSA Company client (as applicable), on the other hand.

A.6.4 Personal Information

In the event that CPSA receives Personal Information from PCI SSC or any Member or CPSA Company client in the course of providing Services or otherwise in connection with this Agreement, in addition to the obligations set forth elsewhere in this Agreement, CPSA will at all times during the Term (as defined in Section A.9.1) maintain such data-protection handling practices as may be required by PCI SSC from time to time, including without limitation, as a minimum, physical, electronic, and procedural safeguards designed: (i) to maintain the security and confidentiality of such Personal Information (including, without limitation, encrypting such Personal Information in accordance with applicable Participating Payment Brand guidelines, if any); (ii) to protect against any anticipated threats or hazards to the security or integrity of such information; and (iii) to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the natural persons to whom such Personal Information relates. CPSA will make available to PCI SSC and the Participating Payment Brands, and will require in its agreements with CPSA Company clients that CPSA Company clients will make so available, such appropriate reviews and reports to monitor CPSA's compliance with the foregoing commitments as PCI SSC or any Participating Payment Brand may reasonably request from time to time. Without limitation of the foregoing, CPSA acknowledges and agrees that if it performs the Services or any other services for PCI SSC, any Participating Payment Brand or any CPSA Company client in a manner that will result in the storage, processing, or transmission of data to which any of the PCI Card Production Security Requirements applies, CPSA shall be required to be certified as compliant with the PCI Card Production Security Requirements as such may be modified by PCI SSC from time to time. If compliance with the PCI Card Production Security Requirements is required, CPSA, at its sole cost and expense, shall: (i) conduct or have conducted the audits required for such compliance; and (ii) take all actions required for CPSA to maintain such compliance. If required to be compliant with any of the PCI Card Production Security Requirements, CPSA acknowledges that it further has the obligation to keep up to date on any changes thereto and implement any required changes.

A.6.5 Return

Within fourteen (14) days after notice of termination of this Agreement or demand by PCI SSC, CPSA promptly shall return to PCI SSC all property and Confidential Information of PCI SSC and of all third parties to the extent provided or made available by PCI SSC; provided, however, that CPSA may retain copies of Confidential Information of PCI SSC to the extent the same were, prior to such notice of termination or demand, either automatically generated archival copies or incorporated into CPSA's workpapers as a result of providing services to a CPSA Company client; and CPSA shall continue to maintain the confidentiality of all such retained Confidential Information in accordance with this Agreement. If agreed by PCI SSC, CPSA may instead destroy all such materials and information and provide a certificate of destruction to PCI SSC, with sufficient detail regarding the items destroyed, destruction date, and assurance that all copies of such information and materials also were destroyed.

A.6.6 Remedies

In the event of a breach of Section A.6.2 by the Receiving Party, the Receiving Party acknowledges that the Disclosing Party will likely suffer irreparable damage that cannot be fully remedied by monetary damages. Therefore, in addition to any remedy that the Disclosing Party may possess pursuant to applicable law, the Disclosing Party retains the right to seek and obtain injunctive relief against any such breach in any court of competent jurisdiction. In the event any such breach results in a claim by any third party, the Receiving Party shall indemnify, defend, and hold harmless the Disclosing Party from any claims, damages, interest, attorney's fees, penalties, costs, and expenses arising out of such third-party claim(s).

A.7 Indemnification and Limitation of Liability

A.7.1 Indemnification

CPSA shall defend, indemnify, and hold harmless PCI SSC and its Members, and their respective subsidiaries, and all affiliates, subsidiaries, directors, officers, employees, agents, representatives, independent contractors, attorneys, successors, and assigns of any of the foregoing (collectively, including without limitation, PCI SSC and its Members, "Indemnified Parties") from and against any and all claims, losses, liabilities, damages, suits, actions, government proceedings, taxes, penalties or interest, associated auditing, and legal expenses and other costs (including without limitation, reasonable attorney's fees and related costs) that arise or result from any claim by any third party with respect to CPSA's (i) breach of its agreements, representations or warranties contained in this Agreement; (ii) participation in the CPSA Program or use of any PCI Materials or CPSA Program-related information (a) in violation of this Agreement or (b) in violation of any applicable law, rule, or regulation; (iii) non-performance of Services for any CPSA Company client that has engaged CPSA to perform Services, including without limitation claims asserted by CPSA Company clients or Members; (iv) negligence or willful misconduct in connection with the CPSA Program, this Agreement, or CPSA's performance of Services, except to the extent arising out of negligence or willful misconduct of an Indemnified Party; or (v) breach, violation, infringement, or misappropriation of any third-party Intellectual Property Right. All indemnities provided for under this Agreement shall be paid by CPSA as incurred by the Indemnified Party. This indemnification shall be binding upon CPSA and its executors, heirs, successors, and assigns. Nothing in this Agreement shall be construed to impose any indemnification obligation on CPSA to the extent the corresponding claim or liability arises solely from a defect in the PCI Materials provided by an Indemnified Party and such PCI Materials are used by CPSA without modification and in accordance with all then applicable publicly available updates, guidance, and best practices provided by PCI SSC.

A.7.2 Indemnification Procedure

CPSA's indemnity obligations are contingent on the Indemnified Party's providing notice of the claim or liability to CPSA, provided that the failure to provide any such notice shall not relieve CPSA of such indemnity obligations except and to the extent such failure has materially and adversely affected CPSA's ability to defend against such claim or liability. Upon receipt of such notice, CPSA will be entitled to control, and will assume full responsibility for, the defense of such matter. PCI SSC will cooperate in all reasonable respects with CPSA, at CPSA's expense, in the investigation, trial and defense of such claim or liability and any appeal arising there from; provided, however, that PCI SSC and/or its Members may, at their own cost and expense, participate in such investigation, trial and defense, and any appeal arising therefrom or assume

the defense of any Indemnified Party. In any event, PCI SSC and/or its Members will each have the right to approve counsel engaged by CPSA to represent any Indemnified Party affiliated therewith, which approval shall not be unreasonably withheld. CPSA will not enter into any settlement of a claim that imposes any obligation or liability on PCI SSC or any other Indemnified Party without the express prior written consent of PCI SSC or such Indemnified Party, as applicable.

A.7.3 No Warranties; Limitation of Liability

(a) PCI SSC PROVIDES THE PCI CARD PRODUCTION SECURITY REQUIREMENTS, THE CPSA PROGRAM, THE CPSA QUALIFICATION REQUIREMENTS, THE WEBSITE, AND ALL RELATED AND OTHER MATERIALS PROVIDED OR OTHERWISE MADE ACCESSIBLE BY PCI SSC IN CONNECTION WITH THE PCI CPSA PROGRAM (THE FOREGOING, COLLECTIVELY, THE "PCI MATERIALS") ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND. CPSA ASSUMES THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE ARISING OUT OF ITS USE OF ANY OF THE PCI MATERIALS.

(b) PCI SSC MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, THE CPSA PROGRAM, THE PCI MATERIALS, OR ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE CPSA PROGRAM. PCI SSC SPECIFICALLY DISCLAIMS, AND CPSA EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THIS AGREEMENT, THE CPSA PROGRAM, THE PCI MATERIALS, ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE CPSA PROGRAM, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITATION OF THE FOREGOING, PCI SSC SPECIFICALLY DISCLAIMS, AND CPSA EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE PCI MATERIALS AND ANY INTELLECTUAL PROPERTY RIGHTS SUBSISTING THEREIN OR IN ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL EXPRESS OR IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, OR SUITABILITY FOR ANY PURPOSE RELATING TO ANY OF THE FOREGOING. THE FOREGOING DISCLAIMER IS MADE BY PCI SSC FOR ITSELF AND, WITH RESPECT TO EACH SUCH DISCLAIMER, ON BEHALF OF ITS LICENSORS AND MEMBERS.

(c) In particular, without limiting the foregoing, CPSA acknowledges and agrees that the accuracy, completeness, sequence, or timeliness of the PCI Materials or any portion thereof cannot be guaranteed. In addition, PCI SSC makes no representation or warranty whatsoever, expressed or implied, and assumes no liability, and shall not be liable in any respect to CPSA regarding (i) any delay or loss of use of any of the PCI Materials, or (ii) system performance and effects on or damages to software or hardware in connection with any use of the PCI Materials.

(d) EXCEPT FOR DAMAGES CAUSED BY THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY, AND EXCEPT FOR THE OBLIGATIONS OF CPSA UNDER SECTIONS A.5 OR A.6, IN NO EVENT SHALL EITHER PARTY OR ANY MEMBER BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES, HOWEVER CAUSED, WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EVEN

IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY DOES NOT APPLY TO INDEMNIFICATION OWED TO AN INDEMNIFIED PARTY PURSUANT TO THIS SECTION A.7.

(e) PCI SSC shall be liable vis-à-vis CPSA only for any direct damage incurred by CPSA as a result of PCI SSC's gross negligence (contractual or extra-contractual) under this Agreement provided PCI SSC's aggregate liability for such direct damage under and for the duration of this Agreement will never exceed the fees paid by CPSA to PCI SSC under Section A.4.

(f) Except as otherwise expressly provided in this Agreement, neither PCI SSC nor any Participating Payment Brand shall be liable vis-à-vis CPSA for any other damage incurred by CPSA under this Agreement or in connection with the CPSA Program, including but not limited to, loss of business, revenue, goodwill, anticipated savings, or other commercial or economic loss of any kind arising in any way out of the use of the CPSA Program (regardless of whether such damages are reasonably foreseeable or PCI SSC has been advised of the possibility of such damages), or for any loss that results from force majeure.

A.7.4 Insurance

At all times while this Agreement is in effect, CPSA shall maintain insurance in such amounts, with such insurers, coverages, exclusions and deductibles which, at a minimum, meet the applicable insurance requirements for U.S. or European Union CPSA Companies (as applicable) participating in the CPSA Program, including without limitation, the insurance requirements for CPSA Companies set forth in Appendix B of the CPSA Qualification Requirements. CPSA acknowledges and agrees that if it is a non-U.S. and non-European Union CPSA Company, unless otherwise expressly agreed by PCI SSC in writing, at all times while this Agreement is in effect, CPSA shall maintain insurance in such amounts, with such insurers, coverages, exclusions, and deductibles that PCI SSC determines, in its sole discretion, is substantially equivalent to the insurance required by PCI SSC for U.S. and European Union CPSA Companies participating in the CPSA Program. CPSA hereby represents and warrants that it meets all applicable insurance requirements as provided for in this Section and that such insurance shall not be cancelled or modified without giving PCI SSC at least twenty (20) days' prior written notice. PCI SSC may modify its insurance requirements from time to time based on parameters affecting risk and financial capability that are general to CPSA Companies or specific to CPSA, provided that PCI SSC is under no obligation to review and does not undertake to advise CPSA on the adequacy of CPSA's insurance coverage.

A.8 Independence; Representations and Warranties

CPSA agrees to comply with all applicable CPSA Qualification Requirements, including without limitation, all requirements and provisions regarding independence, and hereby warrants and represents that CPSA is now, and shall at all times during the Term, remain in compliance with all such CPSA Qualification Requirements. CPSA represents and warrants that by entering into this Agreement it will not breach any obligation to any third party. CPSA represents and warrants that it will comply with all applicable laws, ordinances, rules, and regulations in any way pertaining to this Agreement or its performance of the Services or its obligations under this Agreement.

A.9 Term and Termination

A.9.1 Term

This Agreement shall commence as of the Effective Date and, unless earlier terminated in accordance with this Section A.9, continue for an initial term of one (1) year (the "Initial Term") and thereafter, for additional subsequent terms of one year (each a "Renewal Term" and together with the Initial Term, the "Term"), subject to CPSA's successful completion of all applicable requalification requirements for each Renewal Term.

A.9.2 Termination by CPSA

CPSA may terminate this Agreement at any time upon thirty (30) days' written notice to PCI SSC. Notwithstanding Section A.10.1 below, any notice or other written communication (including by electronic mail) from CPSA pursuant to which or to the effect that CPSA requests, notifies, elects, opts, chooses, decides, or otherwise indicates its desire to cease participation in the CPSA Program, be removed from the CPSA List or terminate this Agreement shall be deemed to constitute notice of termination of this Agreement, and the corresponding Qualification(s), by CPSA pursuant to this Section, and thereafter, notwithstanding the thirty (30) day notice period provided for in the preceding sentence and without any further action by CPSA, PCI SSC may immediately remove CPSA from the CPSA List(s) and may terminate this Agreement effective upon written notice to CPSA.

A.9.3 Termination by PCI SSC

PCI SSC may terminate this Agreement effective as of the end of the then-current Term by providing CPSA with written notice of its intent to terminate or not to renew this Agreement at least sixty (60) days prior to the end of the then-current Term. Additionally, PCI SSC may terminate this Agreement: (i) with written notice upon CPSA's voluntary or involuntary bankruptcy, receivership, reorganization dissolution or liquidation under state or federal law that is not otherwise dismissed within thirty (30) days; (ii) with written notice upon CPSA's breach of any representation or warranty under this Agreement; (iii) with fifteen (15) days' prior written notice following CPSA's breach of any other term or provision of this Agreement (including without limitation, CPSA's failure to comply with any of the CPSA Requirements), provided such breach remains uncured when such 15-day period has elapsed; (iv) in accordance with Section A.9.5 below; (v) if PCI SSC ceases to operate the CPSA Program, whether with or without replacing it with any other program; or (vi) if PCI SSC determines in its sole discretion that remaining a party hereto or performing any of its obligations hereunder has caused, will cause, or is likely to cause PCI SSC to violate any applicable statute, law, regulation, or other legal or regulatory requirement.

A.9.4 Effect of Termination

Upon any termination or expiration of this Agreement: (i) CPSA will be removed from the CPSA List; (ii) CPSA shall immediately cease all advertising and promotion of its Qualification and status as a CPSA Company and its listing(s) on the CPSA List, and ensure that it and its employees do not state or imply that any employee of CPSA is a "CPSA Employee," a "CPSA" or otherwise qualified by PCI SSC under the CPSA Program; (iii) CPSA shall immediately cease soliciting for and performing all Services (including but not limited to processing of Card Production ROCs), provided that CPSA shall complete any and all Services contracted with CPSA Company clients prior to such expiration or the notice of termination if and to the extent instructed by PCI SSC in writing; (iv) to the extent CPSA is instructed to complete any Services pursuant to preceding clause (iii), CPSA will deliver all corresponding outstanding Card Production ROCs and other corresponding reports within the time contracted with the CPSA Company client, (v) CPSA shall remain responsible for all of the obligations, representations, and warranties hereunder with respect to all Card Production ROCs and other corresponding reports submitted by CPSA to PCI SSC or any other person or entity; (vi) CPSA shall return or destroy all PCI SSC and third-party property and Confidential Information in accordance with the terms of Section A.6; (vii) if requested by PCI SSC, CPSA shall obtain (at CPSA's sole cost and expense) the services of a replacement CPSA Company acceptable to PCI SSC for purposes of completing those Services for which CPSA was engaged in its capacity as a CPSA Company prior to such expiration or the notice of termination but which CPSA has not been instructed to complete pursuant to Section (iii) above; (viii) CPSA shall, within fifteen (15) days of such expiration or the notice of termination, in a manner acceptable to PCI SSC, notify those of its CPSA Company clients with which CPSA is then engaged to perform any PCI Card Production Assessment or other Services of such expiration or termination; (ix) if requested by PCI SSC, CPSA shall within fifteen (15) days of such request, identify to PCI SSC in writing all CPSA Company clients with which CPSA was engaged to perform Services immediately prior to such expiration or notice of termination and the status of such Services for each; and (x) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, CPSA Company clients or others of such expiration or termination and the reason(s) therefor. The provisions of Sections A.5.4, A.6, A.7, A.9.4 and A.10 of this Agreement shall survive the expiration or termination of this Agreement for any or no reason.

A.9.5 Revocation

(a) Without limiting the rights of PCI SSC as set forth elsewhere in this Agreement, in the event that PCI SSC determines in its sole but reasonable discretion that CPSA meets any condition for revocation of its Qualification as a CPSA Company as established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions identified as or described as examples of Violations herein or in the CPSA Qualification Requirements, PCI SSC may, effective immediately upon notice of such Violation to CPSA, revoke such Qualification from CPSA ("Revocation"), and such revoked Qualification shall be subject to reinstatement pending a successful appeal in accordance with Section A.9.5(b) below and PCI SSC policies and procedures.

(b) In the event of any Revocation: (i) CPSA will be removed from the CPSA List(s) and/or its listing(s) thereupon may be annotated as PCI SSC deems appropriate; (ii) upon revocation of Qualification as a CPSA Company, CPSA must comply with Section A.9.4 above in the manner otherwise required if this Agreement had been terminated as of the effective date of such Revocation; (iii) CPSA will have a period of thirty (30) days from the date CPSA is given notice of such Violation to submit its written request for appeal to the CPSA Program Manager; (iv) CPSA shall, within fifteen (15) days of such Revocation, in a manner acceptable to PCI SSC, provide notice of such Revocation to those of its CPSA Company clients with which CPSA is then engaged to perform any PCI Card Production Assessment or other Services for which such revoked Qualification is required and, if applicable, of any conditions, restrictions or requirements of such Revocation that may impact its ability to perform such PCI Card Production Assessment or other Services for such CPSA Company clients going forward; and (v) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, CPSA Company clients, or others of such Revocation and the reason(s) therefor. In the event CPSA fails to submit a request for appeal within the allotted 30-day period or such request is denied, this Agreement shall automatically terminate and CPSA's right to such appeal shall be forfeited effective immediately as of the end of such period or such denial, as applicable.

(c) All Revocation appeal proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time for the CPSA Program, PCI SSC will review all relevant evidence submitted by CPSA and each complainant (if any) in connection with therewith, and PCI SSC shall determine whether termination of CPSA's Qualification is warranted or, in the alternative, no action, or specified remedial actions shall be required. All determinations of PCI SSC regarding Revocation and any related termination or appeals shall be final and binding upon CPSA. If PCI SSC determines that termination is warranted, then effective immediately and automatically upon such determination, such Qualification and this Agreement shall terminate. If PCI SSC determines that such termination is not warranted, the Revocation shall be lifted, such Qualification shall be reinstated, and the listing of CPSA that was removed from the CPSA List as a result of such Revocation shall be reinstated. If PCI SSC determines that remedial action is required, PCI SSC shall notify CPSA and may establish a date by which such remedial action must be completed; provided, however, that unless otherwise agreed by PCI SSC in writing the Revocation shall not be lifted, and CPSA shall not be reinstated on the CPSA List, unless and until such time as CPSA has completed such remedial action; and provided, further, that if CPSA fails to complete any required remedial actions by the date (if any) established by PCI SSC for completion thereof, PCI SSC may terminate such Qualification and this Agreement, effective immediately as of or any time after such date.

A.10 General Terms

A.10.1 Notices

All notices required under this Agreement shall be in writing and shall be deemed given when delivered (a) personally, (b) by overnight delivery upon written verification of receipt, (c) by facsimile or electronic mail transmission upon electronic transmission confirmation or delivery receipt, or (d) by certified or registered mail, return receipt requested, five (5) days after the date of mailing. Notices from PCI SSC to CPSA shall be sent to the attention of the Primary Contact named, and at the location specified, on the signature page of this Agreement. Notices from CPSA to PCI SSC shall be sent to the PCI SSC signatory identified on the signature page of this Agreement, at 401 Edgewater Place, Suite 600, Wakefield, Massachusetts 01880. A party may change its addressee and address for notices by giving notice to the other party pursuant to this Section A.10.1. Notwithstanding (and without limitation of) the foregoing: (i) any notice from PCI SSC to CPSA hereunder may be given and shall be deemed to have been effectively delivered in writing when posted to the secure portal designated or reserved by PCI SSC for the CPSA Program(s); and (ii) any notice from PCI SSC to CPSA of any change in Fees may be given and shall be deemed to have been effectively delivered in writing when posted to the PCI SSC Program Fee Schedule on the Website.

A.10.2 Audit and Financial Statements

(a) CPSA shall allow PCI SSC or its designated agents access during normal business hours throughout the Term and for six (6) months thereafter to perform audits of CPSA's facilities, operations and records of Services to determine whether CPSA has complied with this Agreement. CPSA also shall provide PCI SSC or its designated agents during normal business hours with books, records and supporting documentation adequate to evaluate CPSA's performance hereunder. Upon request, CPSA shall provide PCI SSC with a copy of its most recent audited financial statements or those of its parent company which include financial results of CPSA, a letter from CPSA's certified public accountant, or other documentation acceptable to PCI SSC setting out CPSA's current financial status and warranted by CPSA to be complete and accurate. PCI SSC acknowledges that any such statements that are non-public are Confidential Information and shall restrict access to them in accordance with the terms of this Agreement.

(b) Notwithstanding anything to the contrary in Section A.6 of this Agreement, in order to assist in ensuring the reliability and accuracy of CPSA's PCI Card Production Assessments, CPSA hereby agrees to comply with all quality-assurance procedures and requirements established or imposed by PCI SSC from time to time in connection with the CPSA Program (including but not limited to conditions and requirements imposed in connection with remediation, revocation, or any other Qualification status) and that, within 15 days of any written request by PCI SSC, CPSA hereby agrees to provide to PCI SSC such Assessment Results and Related Materials (defined below) as PCI SSC may reasonably request with respect to any CPSA Company client for which CPSA has performed a PCI Card Production Assessment. Each agreement between CPSA and each of its CPSA Company clients (each a “Client Agreement”) shall include such provisions as may be necessary or appropriate, or otherwise required by PCI SSC, to ensure that CPSA has all rights, licenses, and other permissions necessary for CPSA to comply with its obligations and requirements pursuant to this Agreement, with no conditions, qualifications or other terms (whether in such Client Agreement or otherwise) that might tend to nullify, impair, or render unenforceable CPSA’s

right to disclose such Assessment Results and Related Materials as required by this Section. Any failure of CPSA to comply with this Section A.10.2 shall be deemed to be a breach of CPSA's representations and warranties under this Agreement for purposes of Section A.9.3, and upon any such failure, PCI SSC may terminate CPSA's Qualification as a CPSA Company, remove CPSA's name from the CPSA List and/or terminate this Agreement in its sole discretion, upon notice to CPSA. For purposes of the foregoing, "Assessment Results and Related Materials" means: (1) all Card Production ROCs, AOVs, and related or similar information, reports, materials, and assessment results generated and/or obtained in connection with CPSA's performance of PCI Card Production Assessments, including without limitation, all workpapers, notes, and other materials and information generated or obtained in connection therewith in any form, and (2) complete and accurate copies of the provisions of each Client Agreement that relate to or otherwise impact CPSA's ability to comply with its disclosure obligations pursuant to this Agreement; provided that, in each case: (A) any materials otherwise required to be provided to PCI SSC pursuant to this Section may (or shall, as the case may be) be redacted to the extent necessary to comply with applicable law and/or permitted pursuant to PCI SSC policies and procedures, including but not limited to redaction of information regarding pricing, delivery process, and/or confidential and proprietary information of the CPSA Company client (and/or its customers) if such redaction is in accordance with PCI SSC policy, does not eliminate or obscure any language (or the intent or meaning thereof) that may tend to nullify, impair, or render unenforceable CPSA's right to disclose Assessment Results and Related Materials to PCI SSC as required by this Section, and is as limited as reasonably possible; and (B) upon request, CPSA shall provide to PCI SSC a written certification that such redaction complies with preceding clause (A) executed by an officer of CPSA.

A.10.3 Governing Law; Severability

Any dispute in any way arising out of or in connection with the interpretation or performance of this Agreement, which cannot be amicably settled within thirty (30) days of the written notice of the dispute given to the other party by exercising the best efforts and good faith of the parties, shall be finally settled by the courts of Delaware (United States of America) in accordance with Delaware law without resort to its conflict of laws provisions. Each of the parties irrevocably submits to the nonexclusive jurisdiction of the United States District Courts for the State of Delaware and the local courts of the State of Delaware and waives any objection to venue in said courts. Should any individual provision of this Agreement be or become void, invalid, or unenforceable, the validity of the remainder of this Agreement shall not be affected thereby and shall remain in full force and effect, in so far as the primary purpose of this Agreement is not frustrated.

A.10.4 Entire Agreement; Modification; Waivers

The parties agree that this Agreement, including the CPSA Qualification Requirements and any other documents, addenda, supplements, amendments, appendices, exhibits, schedules, or other materials incorporated herein by reference (each of which is hereby incorporated into and made a part of this Agreement by this reference), is the exclusive statement of the agreement between the parties with respect to the subject matter hereof, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties with respect to such subject matter (including without limitation, if applicable, each prior *Card Production Security Assessor (CPSA) Agreement* between CPSA and PCI SSC). This Agreement may be modified, altered or amended only (i) by written instrument duly executed by both parties

or (ii) by PCI SSC upon thirty (30) days' written notice to CPSA, provided, however, that if CPSA does not agree with such unilateral modification, alteration, or amendment, CPSA shall have the right, exercisable at any time within the aforementioned thirty (30) day period, to terminate this Agreement upon written notice of its intention to so terminate to PCI SSC. Any such unilateral modification, alteration, or amendment will be effective as of the end of such 30-day period unless the Agreement is earlier terminated by CPSA pursuant to the preceding sentence. The waiver or failure of either party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of any further right under this Agreement.

A.10.5 Assignment

CPSA may not assign this Agreement, or assign, delegate, or subcontract any of its rights and/or obligations under this Agreement.

A.10.6 Independent Contractors

The parties to this Agreement are independent contractors and neither party shall hold itself out to be, nor shall anything in this Agreement be construed to constitute either party as the agent, representative, employee, partner, or joint venture of the other. Neither party may bind or obligate the other without the other party's prior written consent.

A.10.7 Remedies

All remedies in this Agreement are cumulative, in addition to and not in lieu of any other remedies available to either party at law or in equity, subject only to the express limitations on liabilities and remedies set forth herein.

A.10.8 Counterparts

This Agreement may be signed in two or more counterparts, any or all of which may be executed by exchange of facsimile and/or electronic transmission, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

A.10.9 Conflict

In the event of any express conflict or inconsistency between the terms and provisions of this Agreement and terms and provisions of the CPSA Qualification Requirements, this Agreement shall control. Any and all disputes or disagreements regarding any such conflict or inconsistency shall be resolved by PCI SSC in its sole but reasonable discretion, and all determinations of PCI SSC in this regard shall be final and binding.

A.10.10 No Third-Party Beneficiaries

Except as expressly provided herein, the provisions of this Agreement are for the benefit of the parties hereto only, no third-party beneficiaries are intended, and no third party may seek to enforce or benefit from the provisions hereof.

Appendix B: Insurance Coverage

Prior to the commencement of the Services under the CPSA Agreement, the CPSA Company ("Security Assessor") shall procure the following insurance coverage, at its own expense, with respect to the performance of such Services. Such insurance shall be issued by financially responsible and properly licensed insurance carriers in the jurisdictions where the Services are performed and rated at least A VIII by *Best's Rating Guide* (or otherwise acceptable to PCI SSC) and with minimum limits as set forth below. Such insurance shall be maintained in full force and effect for the duration of this agreement and any renewals thereof:

- WORKERS' COMPENSATION: Statutory Workers Compensation as required by applicable law and
- EMPLOYER'S LIABILITY with a limit of $1,000,000
- COMMERCIAL GENERAL LIABILITY INSURANCE including PRODUCTS, COMPLETED OPERATIONS, ADVERTISING INJURY, PERSONAL INJURY, and CONTRACTUAL LIABILITY INSURANCE with the following minimum limits for Bodily Injury and Property Damage on an Occurrence basis: $1,000,000 per occurrence and $2,000,000 annual aggregate. PCI SSC to be added as "Additional Insured." The policy Coverage Territory must include the entire Region(s) in which the CPSA Company has qualified to operate.
- COMMERCIAL AUTOMOBILE INSURANCE including owned, leased, hired, or non-owned autos subject to minimum limits of $1,000,000 per accident
- CRIME/FIDELITY BOND including first-party employee dishonesty, robbery, fraud, theft, forgery, alteration, mysterious disappearance, and destruction. Coverage must also include third-party employee dishonesty – i.e., coverage for claims made by the CPSA Company's client against the CPSA Company for theft committed by the CPSA Company's employees. The minimum limit shall be $1,000,000 each loss and annual aggregate. The policy Coverage Territory must include the entire Region(s) in which the CPSA Company is qualified to operate.
- TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE covering liabilities for financial loss resulting or arising from acts, errors, or omissions in rendering computer or information technology Services, or from data damage/destruction/corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service, and loss of income from network security failures in connection with the Services provided under this agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate. The policy Coverage Territory must include the entire Region(s) in which the CPSA Company is qualified to operate.

If any of the above insurance is written on a claims-made basis, then Security Assessor shall maintain such insurance for five (5) years after the termination of this agreement. The limits shown in the appendix may be written in other currencies, but should be the equivalent of the limits in US dollars shown here.

Without limiting Security Assessor's indemnification duties as outlined in the Indemnification Section herein, PCI SSC shall be named as an additional insured under the Commercial General Liability for any claims and losses arising out of, allegedly arising out of, or in any way connected to the Security Assessor's performance of the Services under this agreement. The insurers shall agree that the Security

Assessor's insurance is primary, and any insurance maintained by CPS SSC shall be excess and non-contributing to the Security Assessor's insurance.

Prior to commencing of services under this agreement and annually thereafter, Security Assessor shall furnish a certificate, satisfactory to PCI SSC from each insurance company evidencing that the above insurance is in force in compliance with the terms of this insurance section, stating policy numbers, dates of expiration, and limits of liability, and further providing that Security Assessor will endeavor to provide at least thirty (30) days' prior written notice in the event the insurance is canceled. In addition to the certificate of insurance, Security Assessor shall provide copies of the actual insurance policies if requested by PCI SSC at any time. Security Assessor shall send Certificate(s) of Insurance confirming such coverage according to the directions in Section 2.3 of this document. Fulfillment of obligations to procure insurance shall not otherwise relieve Security Assessor of any liability hereunder or modify Security Assessor's obligations to indemnify PCI SSC.

WAIVER OF SUBROGATION: Security Assessor agrees to waive subrogation against PCI SSC for any injuries to its employees arising out of or in any way related to Security Assessor's performance of the Service under this agreement. Further, Security Assessor agrees that it shall ensure that the Workers' Compensation/Employer's Liability insurers agree to waive subrogation rights, in favor of PCI SSC, for any claims arising out of or in any way connected to Security Assessor's performance of the Services under this agreement.

Appendix C: CPSA Company Application

Please provide the information requested in Section 1 below, check each applicable box and complete the fields in Sections 2–4 below, and sign where indicated at the end of this CPSA Company Application.

☐ The Company certifies it is currently a PCI QSA Company in Good Standing.
(Take note of form items with a footnote[1] indicated.)

Applicant CPSA Company (the "Company") Information – Section 1					
Company Name:					
Primary Contact Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP/Postal Code:	
QA Contact Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP/Postal Code:	
Secondary Contact Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP/Postal Code:	
URL:					

☐ The Company acknowledges and agrees that in order to participate as a CPSA Company in the CPSA Program, it must satisfy all of the requirements specified in the CPSA Qualification Requirements and supporting documents.

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Company Business Requirements – Section 2
☐ The Company acknowledges the minimum business requirements and related information that must be provided to PCI SSC regarding the Company's business legitimacy, independence, and required insurance coverage pursuant to Section 2 of the CPSA Qualification Requirements, and agrees to comply with such requirements.
Business Legitimacy – 2.1.2 Provisions
☐ The Company certifies that it is a legal entity.
☐ The Company certifies that it is providing to PCI SSC herewith a copy of its current formation document or equivalent (the "Business License"). (Refer to the Documents Library on the Website – *Business License Requirements* for more information.) [1]
Year of incorporation/formation of Company[1]:
Regions where services will be offered: Asia-Pacific, Canada, CEMEA (Central Europe, Middle East, Africa) Europe, LAC (Latin America, Caribbean), USA:
Describe any past or present allegations or convictions of any fraudulent or criminal activity involving the company (and/or company principals), and the status and resolution[1]:
Describe any past or present appeals or revocations of any qualification issued by PCI SSC to the Company (or any predecessor entity or, unless prohibited by applicable law, any CPSA Employee of any of the foregoing), and the current status and any resolution thereof[1]:
Independence – 2.2.2 Provisions
☐ The Company hereby acknowledges and agrees that it must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI Card Production Assessments.
☐ The Company hereby certifies that it has a code-of-conduct policy and agrees to provide that policy to PCI SSC upon request.
☐ The Company hereby agrees to adhere to all independence requirements as established by PCI SSC, including without limitation, all items listed in Section 2.2.1 of the CPSA Qualification Requirements.
☐ Below or attached hereto are (a) a description of the Company's practices for maintaining and assuring assessor independence, including but not limited to, the Company's practices, organizational structures, separation of duties, rules, and employee education in place to prevent conflicts of interest, and (b) copies of all written Company policies relating to any of the foregoing.[1]
(Continued)

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Company Business Requirements – Section 2 *(Continued)*

☐ The Company hereby:

- Agrees to maintain and adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI Card Production Assessments.
- Agrees to maintain and adhere to a code-of-conduct policy and provide the policy to PCI SSC upon request.
- Agrees to adhere to all independence requirements as established by PCI SSC, including without limitation, all items listed in Section 2.2.1 of the CPSA Qualification Requirements.
- Agrees not to undertake to perform any PCI Card Production Assessment of any entity that it controls, is controlled by, is under common control with, or in which it holds any investment.
- Agrees that it has not and will not have offered or provided (and has not and will not have been offered or received) to (or from) any employee of PCI SSC or any customer, any gift, gratuity, service, or other inducement (other than compensation in an arm's-length transaction), in order to enter into the CPSA Agreement or any agreement with a customer, or to provide CPSA-related services.
- Agrees to fully disclose in the Report on Compliance if the Company assesses any customer that uses any security-related devices or security-related applications that have been developed or manufactured by the Company, or to which the Company owns the rights, or that the Company has configured or manages, including but not limited to the items described in Section 2.2.1 of the CPSA Qualification Requirements.
- Agrees that when any of its CPSA Employees recommends remediation actions that include any solution or product of the Company, the CPSA Employee will also recommend other market options that exist.
- Agrees that the Company has and will maintain separation-of-duties controls in place to ensure that its CPSA Employees conducting PCI Card Production Assessments are independent and not subject to any conflict of interest.
- Agrees that its CPSA Employees will be employed by only one CPSA Company at any given time.
- Agrees not to use its status as a "listed CPSA" to market services unnecessary to bring clients into compliance with the PCI Card Production Security Requirements.
- Agrees not to misrepresent any requirement of the PCI Card Production Security Requirements in connection with its promotion or sales of services to clients, and not to state or imply that the PCI Card Production Security Requirements requires usage of any of the Company's products or services.

Insurance Coverage – 2.3.2 Provisions

☐	The Company agrees that at all times while its CPSA Agreement is in effect, Company will maintain sufficient insurance, insurers, coverage, exclusions, and deductibles that PCI SSC reasonably requests to adequately insure the Company for its obligations and liabilities under the CPSA Agreement, including without limitation the Company's indemnification obligations.
☐	The Company hereby acknowledges and agrees to adhere to all requirements for insurance coverage required by PCI SSC, including without limitation the requirements in Appendix B, "Insurance Coverage," which includes details of required insurance coverage.
☐	The Company hereby certifies to PCI SSC that, along with this application, the Company is providing to PCI SSC a proof-of-coverage statement demonstrating that its insurance coverage matches locally set insurance coverage requirements.[1]
☐	The Company hereby agrees not to subcontract or assign any portion of the CPSA services.

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Company Business Requirements – Section 2 *(Continued)*
☐ A copy of the Company's bound insurance coverage is attached to this application.[11]
Fees – 2.4.1 Requirements
☐ The Company acknowledges that it will be charged a CPSA Company fee and annual fees for each CPSA Employee PCI SSC training.
☐ The Company agrees to pay all such fees upon invoice from PCI SSC (or as part of the CPSA training registration process, if applicable), and that any such fees invoiced by PCI SSC will be made payable to PCI SSC according to instructions provided on the corresponding invoice.
CPSA Agreement – 2.5.1 Requirements
☐ The Company acknowledges and agrees that along with its completed application package it is providing to PCI SSC a CPSA Agreement between PCI SSC and the Company, in unmodified form, signed by a duly authorized officer of the Company.
PCI SSC Code of Professional Responsibility – 3.3.1 Requirements
☐ The Company acknowledges and agrees that it has read and understands the PCI SSC Code of Professional Responsibility, and hereby agrees to advocate, continuously adhere to, and support the terms and provisions thereof.

CPSA Capability Requirements – Section 3
3.1 CPSA Company Services and Experience ***Note:*** *These sections are intended to draw out specific experience about the company. The company must provide examples (including the timeframe) of how its work experience meets the Card Production Security Assessor Program requirements.*
CPSA Company Skills and Experience – 3.1.2 Provisions
☐ The Company represents and warrants that it currently possesses (and at all times while it is a CPSA Company will continue to possess) technical security assessment experience similar or related to PCI Card Production Assessments, and that it has (and must have) a dedicated security practice that includes staff with specific job functions that support the security practice.
☐ The Company acknowledges and agrees that in order to perform or manage any PCI Card Production Assessment it must be qualified by PCI SSC and in Good Standing or in compliance with remediation as a CPSA Company.
☐ The Company acknowledges and agrees that it must fulfill all CPSA Qualification Requirements, all CPSA Company Requirements, and comply with all terms and provisions of the CPSA Agreement, any other agreements executed with PCI SSC, and all other applicable policies and requirements of the CPSA Assessor Program, as mandated or imposed by PCI SSC from time to time, including but not limited to all requirements in connection with PCI SSC's quality-assurance initiatives, remediation, and revocation.
(Continued)

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Capability Requirements – Section 3

CPSA Capability Requirements – Section 3 *(Continued)*

Additional Deliverables for CPSA Companies

Specialization and Company Details

☐ Immediately below is a description of the Company's relevant areas of specialization within information security – for example, network security, database and application security, and incident response – demonstrating at least one area of specialization:

Total number of Company employees on staff:
The number of CPSA Employees expected to perform PCI Card Production Assessments:
Describe any additional evidence of a dedicated security practice within the Company:
Describe other core business offerings:
Languages supported by the applicant CPSA Company:

Attestation that all the above skill sets will be present and fully utilized on every PCI Card Production Assessment:

☐ The Company acknowledges and agrees that all of the above skill sets will be present and fully utilized on every PCI Card Production Assessment.

Two client references from relevant security engagements within the last 12 months[1]:

Client Company Name:		From (date):	To (date):
Contact Name:		Job Title:	
Telephone *or* e-mail:			
State/Province:		Country:	
Client Company Name:		From (date):	To (date):
Contact Name:		Job Title:	
Telephone *or* e-mail:			
State/Province:		Country:	

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Administrative Requirements – Section 4

☐ The Company hereby acknowledges and agrees to the administrative requirements for CPSA Companies set forth in the CPSA Qualification Requirements, including company contacts, background checks, adherence to PCI Card Production procedures, quality assurance, and protection of confidential and sensitive information.

Background Checks – 4.2.2 Provisions

☐ The Company agrees that its policies and hiring procedures must include performing background checks and satisfying the provisions in Section 4.2.2 (to the extent legally permitted within the applicable jurisdiction) when hiring each applicant CPSA Employee.

Below is a summary description of the Company's personnel background check policies[1]:

The Company's personnel background check policies and procedures include the following (*to the extent legally permitted within the applicable jurisdiction*)[1]:

☐ Verification of aliases (when applicable)

☐ Reviewing records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants

☐ Annually review records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants

☐ Minor offenses (for example, misdemeanors or non-US equivalents) are allowed, but major offenses (for example, felonies or non-US equivalents) automatically disqualify an employee from serving as a CPSA Employee

☐ The Company understands and agrees that, upon request, it must provide to PCI SSC the background check history for each of its CPSA Employees, to the extent legally permitted within the applicable jurisdiction.

Internal Quality Assurance – 4.3.2 Provisions

☐ The Company acknowledges and agrees that all quality-assurance reviews must be conducted by personnel qualified by PCI SSC as CPSA Employees or who have completed CPSA Knowledge Training.

☐ The Company understands and agrees that it must annually provide to PCI SSC the completed CPSA Annual QA Questionnaire in the Portal upon request by PCI SSC.

☐ The Company acknowledges and agrees that it must adhere to all quality-assurance requirements described in the CPSA Qualification Requirements and supporting documentation, must have a quality-assurance program, documented in its Quality Assurance manual, and must maintain and adhere to a documented quality-assurance process and manual that includes all items described in Section 4.3.1 of the CPSA Qualification Requirements.

☐ The Company acknowledges and agrees that its internal quality-assurance reviews must be performed by qualified personnel (independent of the assessing and/or authoring CPSA Employee) and must cover assessment procedures performed, supporting documentation, information documented in the Card Production ROC related to the appropriate selection of system components, sampling procedures, remediation recommendations, proper use of payment definitions, consistent findings, and thorough documentation of results.

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Administrative Requirements – Section 4

(Continued)

CPSA Administrative Requirements – Section 4 *(Continued)*

The Company acknowledges and agrees that as a CPSA Company, it must at its sole cost and expense:

- ☐ At all times maintain and adhere to the internal quality-assurance requirements as described in Section 4.3.1 of the CPSA Qualification Requirements.
- ☐ Permit PCI SSC, upon request from time to time, to conduct audits of the Company and/or to conduct site visits.
- ☐ Inform each Company PCI Card Production Assessment client of the CPSA Feedback Form (available on the Website), upon commencement of the PCI Card Production Assessment for that client.
- ☐ Conduct all PCI Card Production Assessments on-site at the applicable client's facilities or remotely according to the *PCI SSC Remote Assessment Guidelines and Procedures.*

Protection of Confidential and Sensitive Information – 4.4.2 Provisions

- ☐ The Company currently has and agrees to adhere to a documented process for protection of confidential and sensitive information, which includes adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.
- ☐ The Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties under the CPSA Agreement, unless (and to the extent) disclosure is expressly permitted thereunder.
- ☐ The Company's confidential and sensitive data protection handling policies and practices include all physical, electronic, and procedural safeguards described in Section 4.4 of the CPSA Qualification Requirements.
- ☐ The Company agrees to provide PCI SSC a blank copy of the confidentiality agreement that it requires each CPSA to sign (include a blank copy of such confidentiality agreement with this application)[1].

Evidence (Workpaper) Retention – 4.5.2 Provisions

- ☐ The Company has an evidence-retention policy and procedures per Section 4.5.1 of the CPSA Qualification Requirements and agrees to retain all records created and/or obtained during each PCI Card Production Assessment for a minimum of three (3) years.
- ☐ The Company has and agrees to adhere to a documented process for securely maintaining digital and/or hard copies of all case logs, Assessment Results, workpapers, notes, and other information created and/or obtained by the Company during each PCI Card Production Assessment.
- ☐ The Company agrees to make the foregoing materials and information available to PCI SSC upon request for a minimum of three (3) years.
- ☐ The Company agrees to provide a copy of the foregoing evidence-retention policy and procedures to PCI SSC upon request.

Security Incident Response – 4.6.2 Provisions

[1] QSA Companies in good standing will have already provided these materials and will not be required to resubmit them as part of the initial CPSA Company application process if there have been no changes to such materials since those materials were last submitted to PCI SSC.

CPSA Administrative Requirements – Section 4 *(Continued)*	
☐	The Company has a security incident-response plan and procedures per Section 4.6 of the CPSA Qualification Requirements and agrees to retain all records created and/or obtained in connection with the discovery and response regarding the applicable Incident for a minimum of three (3) years.
☐	The Company's security incident-response plan includes instructions and procedures for reporting and documenting evidence of each Incident.

CPSA Administrative Requirements – Section 4 *(Continued)*

Signature

By signing below, the undersigned hereby:

(a) Represents and certifies to PCI SSC that (s)he is an officer of the Company and is duly authorized to legally bind the Company to the terms of this CPSA Company Application; and

(b) Both individually and by and on behalf of the Company: (i) represents and certifies that the information provided in this CPSA Company Application is true, correct, and complete; and (ii) acknowledges, accepts, agrees to, and makes the attestations and certifications set forth in (as the case may be) each of the statements checked (or otherwise marked) in this CPSA Company Application above.

Legal Name of Applicant CPSA Company			
Officer:		Title:	
By:			
Duly authorized officer signature ↑		*Date* ↑	

[remainder of page intentionally left blank]

Appendix D: CPSA Employee Application – Logical Controls

For each individual applying for qualification as a CPSA Employee (each a "Candidate") for purposes of performing Logical PCI Card Production Assessments, the CPSA Company or applicant CPSA Company employing such individual (the "Company") must submit to PCI SSC a copy of this CPSA Employee Application, completed and executed by such Candidate.

Company Information					
Company Name:					
Candidate Information					
Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP/Postal Code:	
URL:					

☐ A résumé or CV for the applicant has been submitted along with the application.

CPSA Employee Skills, Experience and Education			
Provide examples of work or a description of the Candidate's experience with cryptography and key management in cryptographic techniques including cryptographic algorithms, key management, and key lifecycle:			
Examples of work or description of the Candidate's experience with *cryptography:* *Describe the types of cryptography the Candidate has used, such as hashing, symmetric, asymmetric, and algorithms used such as Diffie-Hellman, elliptic curve, DES, Blowfish, MD5.*			
From (date):	To (date):	Total time: Years	Months
Examples of work or description of the Candidate's experience with *key management*: *Describe the Candidate's knowledge of implementing key management, for example, key storage, access control, incident response in the event of compromise, and lifecycle management (rotation, destruction, revocation).*			
From (date):	To (date):	Total time: Years	Months
Provide examples of work or a description of the Candidate's knowledge and experience with cryptography and key management:			
Knowledge of industry standards for cryptographic techniques and key management, including but not limited to ISO 11568 and 13491, ANSI X9.24 and X9.97, and NIST 140-2 Level 3: *Describe specific standards with which the Candidate has knowledge and/or experience and how they were used to design solutions, test for compliance, etc.*			
Total time: Years	Months		
Knowledge of Public Key Infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA): *Describe the Candidate's experience with digital certificates. For example, obtaining, generating, and deploying digital certificates, methods to protect or store digital certificates, certificate revocation, etc.*			
Total time: Years	Months		
Knowledge of Hardware Security Modules (HSMs) operations, policies, and procedures: *Describe the Candidate's experience with HSMs. For example, HSM configuration, deployment, use, and developing related policies and procedures.*			
Total time: Years	Months		
Knowledge of POI key-injection systems and techniques including Key Loading Devices (KLDs) and key-management methods, such as "Master/Session Key," "DUKPT": *Describe the Candidate's experience with key injection. For example, types of keys loaded, KLDs, key-management methods, etc.*			
Total time: Years	Months		
Knowledge of physical security techniques for high-security areas: *Describe the Candidate's experience with physically securing systems and rooms. For example, badge systems, entry logs, man-traps, physical keys, etc.*			
Total time: Years	Months		

CPSA Employee Skills, Experience and Education *(Continued)*			
Examples of work and/or description of experience in **network security** (for example, administration of firewalls, intrusion prevention systems, etc.):			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **systems security:**			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **auditing information systems and processes:**			
From (date):	To (date):	Total time: Years	Months

Candidate Professional Certifications (check all that apply):			
☐	(ISC)^2 CISSP	Certification number:	Expiry date:
☐	ISACA CISM	Certification number:	Expiry date:
☐	ISACA CISA	Certification number:	Expiry date:
☐	SANS GIAC/GSNA	Certification number:	Expiry date:
☐	IRCA Auditor	Certification number:	Expiry date:
☐	IIA CIA	Certification number:	Expiry date:
☐	ISO 27001, Lead Auditor/Implementer, Internal Auditor	Certification number: Accredited certification body:	Date achieved:

Note: *"In process" certifications, where the certification number has not yet been issued, do not meet the requirement.*

Signature

By signing below, I hereby acknowledge and agree that:

(a) The information provided above is true, accurate and complete;

(b) I have read and understand the CPSA Qualification Requirements and will comply with the terms thereof; and

(c) I have read and understand the PCI SSC Code of Professional Responsibility, and will advocate, continuously adhere to and support the terms and provisions thereof.

Candidate:		Title:	
Candidate signature ↑		*Date ↑*	

Appendix E: CPSA Employee Application – Physical Controls

For each individual applying for qualification as a CPSA Employee (each a "Candidate") for purposes of performing Physical PCI Card Production Assessments, the CPSA Company or applicant CPSA Company employing such individual (the "Company") must submit to PCI SSC a copy of this CPSA Employee Application, completed and executed by such Candidate.

Company Information					
Company Name:					
Candidate Information					
Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP/Postal Code:	
URL:					

☐ A résumé or CV for the applicant has been submitted along with the application.

CPSA Employee Skills, Experience and Education			
Examples of work and/or description of experience in **Physical Security** (excluding physical security audits).			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **Physical Security Audits:**			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **Systems Security** (logical security of systems that provide or enforce physical security—e.g., CCTV and access control systems):			
From (date):	To (date):	Total time: Years	Months

Candidate Professional Certifications (check all that apply):		
☐ ASIS PSP	Certification number:	Expiry date:
☐ ASIS CPP	Certification number:	Expiry date:
☐ ISACA CISA	Certification number:	Expiry date:
☐ SANS GIAC/GSNA	Certification number:	Expiry date:
☐ IRCA Auditor	Certification number:	Expiry date:
☐ IIA CIA	Certification number:	Expiry date:
☐ ISO 27001, Lead Auditor/Implementer, Internal Auditor	Certification number: Accredited certification body:	Date achieved:

Note: *"In process" certifications, where the certification number has not yet been issued, do not meet the requirement.*

Signature

By signing below, I hereby acknowledge and agree that:

(a) The information provided above is true, accurate and complete;

(b) I have read and understand the CPSA Qualification Requirements and will comply with the terms thereof; and

(c) I have read and understand the PCI SSC Code of Professional Responsibility, and will advocate, continuously adhere to and support the terms and provisions thereof.

Candidate:		Title:	
Candidate signature ↑			*Date ↑*