



Payment Card Industry (PCI) Qualification Requirements

**For Payment Card Industry
Professionals (PCIP)[™]**

Version 2.0

July 2014

Document Changes

Date	Version	Description
September 2012	1.0	Initial version of <i>PCIP Qualification Requirements</i>
November 2012	1.1	Minor modifications to update training and exam time allowances
November 2013	1.1.1	Minor edits to align with PCI DSS and PA-DSS v3.0
July 2014	2.0	Change qualification expiration from two years to three; add clarity to the application process; add new continuing education requirement

Table of Contents

Document Changes	i
1 Introduction	1
1.1 Overview of the PCIP Credential	1
1.2 Benefits of Becoming a PCIP	2
2 Qualification Process	3
2.1 Become Familiar with the PCI Standards and Supporting Documents	3
2.2 Complete and Submit an Application	3
2.3 Agree to Support the PCI Code of Professional Responsibility	4
2.4 Complete the PCIP Training Course	4
2.5 Take and Pass the PCIP Exam	4
2.6 Achieve Qualification	4
2.7 Maintain Qualification	5
3 PCIP Course Description	6
4 Credential Policies	7
4.1 Use of the Credential	7
4.2 Grace Period for Lapsed Qualifications and Credentials	7
4.3 Exam Security	7
4.4 Practitioner Feedback	8
4.5 Suspension and Revocation	8
4.6 Appeals Policy	8
4.7 Privacy Policy	9
Appendix A: PCIP Application	10
Appendix B: Code of Professional Responsibility	15

1 Introduction

The PCI SSC Payment Card Industry Professional (PCIP)[™] Program provides a foundational credential for industry practitioners who demonstrate their professional knowledge and understanding of PCI SSC standards (“PCI Standards”) and supporting materials. The PCI Security Standards Council, LLC (“PCI SSC”) sponsors this qualification and serves as an impartial, third-party evaluator of each candidate’s knowledge and understanding of PCI Standards. PCI SSC is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The purpose of these *Payment Card Industry (PCI) Qualification Requirements for Payment Card Industry Professionals (PCIP)* (the “PCIP Qualification Requirements”) is to provide the information required to apply for PCIP status by summarizing key aspects of the program and steps to earning and maintaining the PCIP credential. Questions about the program should be e-mailed to: pcip@pcisecuritystandards.org.

1.1 Overview of the PCIP Credential

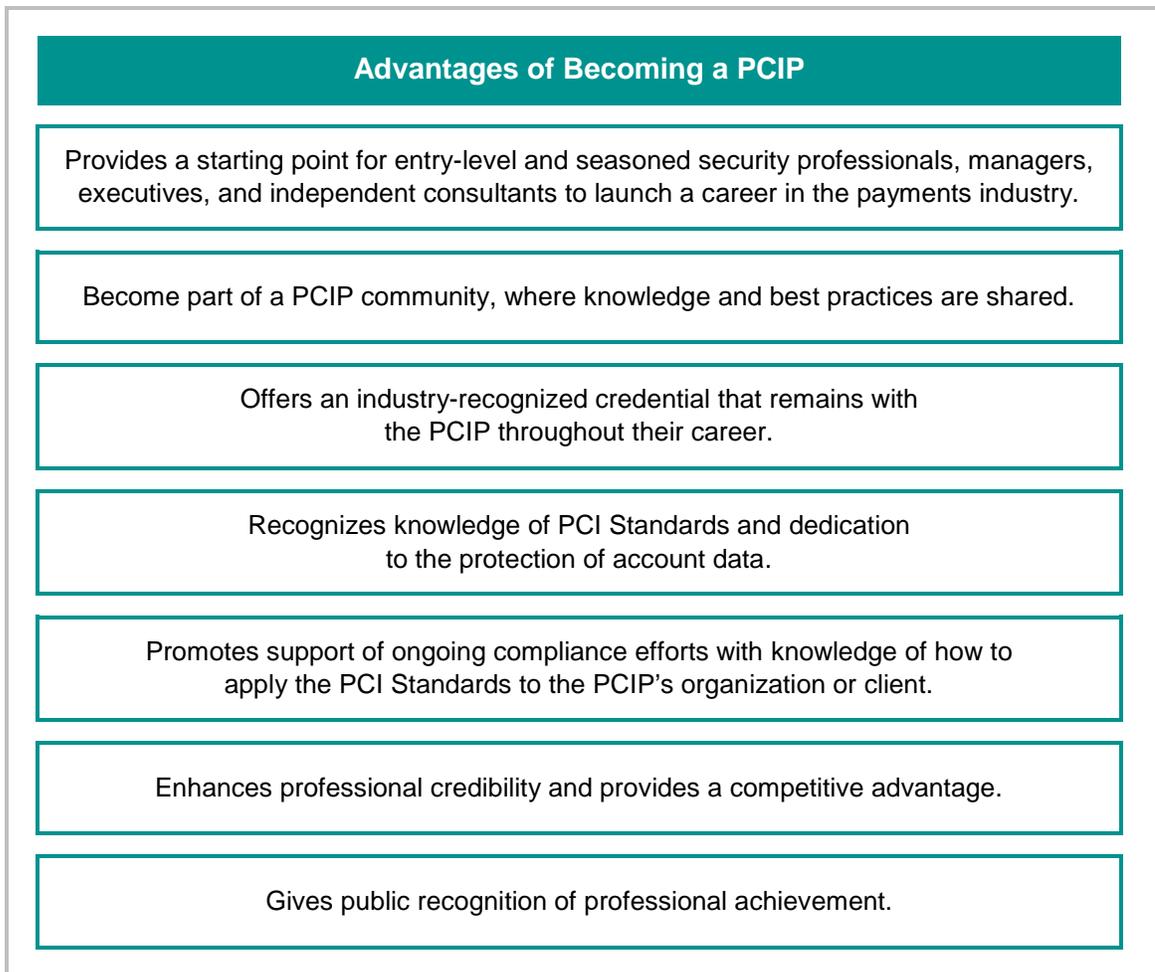
Through the process of becoming a PCIP, the candidate will gain knowledge of the PCI Standards and how they relate to one another. Subject to qualification-renewal requirements, the PCIP credential remains with the individual, which means that as individuals switch employers they are able to maintain the PCIP credential throughout the entirety of their career growth and professional development. Candidates must possess a base level of knowledge and awareness of information technology, network security and architecture, and payment industry participants prior to beginning the process of becoming a PCIP and are strongly encouraged to complete the PCIP training course offered by PCI SSC before taking the PCIP examination.

Note: *Individuals who are qualified and in good standing as QSA employees or ISAs (as defined in the applicable QSA and ISA program materials) throughout the PCIP application process (collectively, “Eligible QSA and ISA Individuals”) may apply for the PCIP credential and qualification without completing PCIP-specific exams or training or reporting the CPE hours required of non-assessor PCIPs, as addressed further below.*

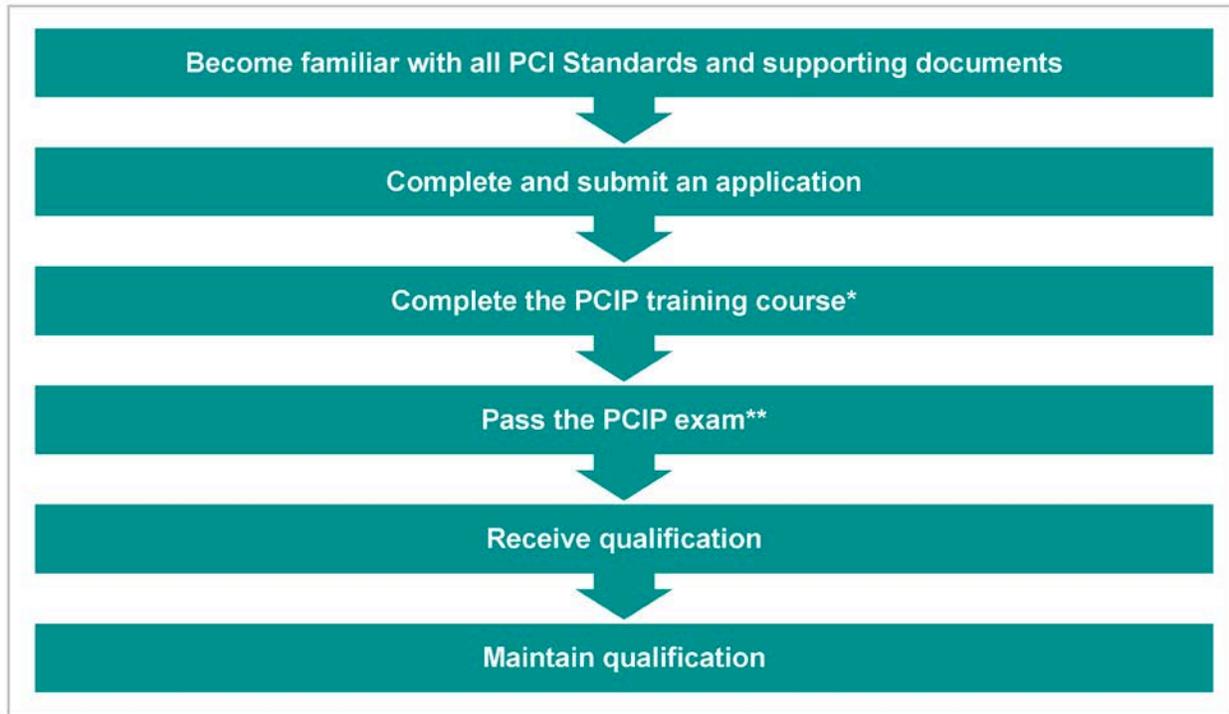
1.2 Benefits of Becoming a PCIP

Becoming a PCIP demonstrates a level of understanding that can provide a strong foundation for a career in the payments security industry. Individuals who may be interested in this program include, but are not limited to, entry-level and seasoned security professionals, managers, executives, application developers, sales engineers, product management and marketing professionals, independent consultants and Eligible QSA and ISA Individuals. PCIP status also indicates a solid foundation for future career progression to other PCI qualifications such as QSA or ISA.

By becoming a PCIP, the applicant is joining other dedicated professionals in the pursuit of the protection of account data and the environments where such information is stored, processed or transmitted.



2 Qualification Process



* Candidates may choose to take the PCIP exam without accessing the PCIP training course.

** Eligible QSA and ISA Individuals are not required to take the PCIP exam.

2.1 *Become Familiar with the PCI Standards and Supporting Documents*

Candidates for PCIP qualification must familiarize themselves with background information regarding the PCI Standards and supporting documents by reviewing the material found on the PCI SSC website at <http://www.pcisecuritystandards.org> (the “PCI SSC Website”).

Candidates are expected to have a good level of awareness of the PCI Standards and more in-depth knowledge of PCI DSS. They should therefore pay particular attention to the *PCI Data Security Standard Requirements and Security Assessment Procedures* before taking the PCIP training and exam.

2.2 *Complete and Submit an Application*

In order to become a PCIP, candidates must first complete and submit an online application and pay applicable PCIP program fees. Fees may be paid by check or other means approved by PCI SSC. Fees to participate in this program (“PCIP Program Fees”) are specified in the current *PCIP Program Fees Schedule* located on the PCI SSC Website.

Candidates must possess a base level of knowledge and awareness of information technology, network security, network architecture, and payment industry participants. As part of the application process candidates must submit their resume or CV evidencing at least 2 years of work experience in an IT or IT-related role. **Note:** *Eligible QSA and ISA Individuals are deemed to have fulfilled this requirement.*

PCI SSC reserves the right to reject any applicant if PCI SSC determines in its reasonable discretion, or has reason to believe, that the applicant fails to satisfy applicable PCIP program requirements or has, within two years prior to the application date, engaged in any conduct that would have entitled PCI SSC to revoke PCIP status.

2.3 Agree to Support the PCI Code of Professional Responsibility

PCI SSC has adopted a *Code of Professional Responsibility* (the “Code”) to help ensure the highest standards of ethical and professional conduct are followed. PCIP candidates must agree to advocate, adhere to, and support the Code. The Code is attached as Appendix B to the *PCIP Qualification Requirements*, and by submitting a PCIP Application to PCI SSC, the PCIP applicant agrees to advocate, adhere to and support the Code.

2.4 Complete the PCIP Training Course

After submitting the application, individuals who have chosen to complete the PCIP training course will be e-mailed instructions for accessing the course when PCI SSC receives the application fee. Please refer to the current schedule of PCIP program fees (the “PCIP Program Fees Schedule”) on the PCI SSC Website for course pricing information. Payment of the course fee allows the candidate a 30-day window to complete the course. Candidates can access the course anytime during this 30-day period.

2.5 Take and Pass the PCIP Exam

Candidates will be given information on scheduling a computer-based PCIP exam at an authorized Pearson VUE Test Center. The Pearson VUE testing network includes over 5,000 testing centers in over 165 countries. The exam must be completed in one sitting and must be taken within 30 days of the candidate being given the information on how to schedule the exam. Eligible QSA and ISA Individuals are deemed to have satisfied the exam requirement.

Candidates taking the exam will receive a pass/fail notification at its conclusion. Candidates who do not pass the exam on the first attempt may retake the exam within 365 days by paying a retake fee. Individuals who are not successful at passing the exam on the second attempt, or do not retake the exam within 365 days, are required to pay the initial course fee before taking the exam again.

2.6 Achieve Qualification

Upon meeting and satisfying all applicable eligibility and exam requirements, the candidate will receive notification of active PCIP status and be assigned a unique number by PCI SSC. Each PCIP will receive an electronic certificate that is suitable for printing and framing. PCIP qualifications are issued for a three-year period, effective on the date that the examination was passed (or for Eligible QSA and ISA Individuals, effective as of the date the PCIP credential is issued by PCI SSC).

No qualification shall be valid if obtained or renewed through fraud or the submission of inaccurate qualification data. The qualification will remain valid as long as the holder meets PCI SSC’s maintenance requirements for PCIPs and complies with the *PCI SSC Code of Professional Responsibility*.

2.7 Maintain Qualification

PCI SSC's maintenance requirements help ensure that PCIPs remain current with technical and industry changes and demonstrate professionalism. To maintain active qualification status, PCIPs must:

- Abide by the *PCI SSC Code of Professional Responsibility*.
- Pass a PCIP requalification examination every three years (or maintain QSA employee or ISA qualification in good standing).
- Pay the required maintenance fee as specified in the current PCIP Program Fees Schedule located on the PCI SSC Website.
- Provide proof of information technology or payment card industry education of a minimum 10 Continuing Professional Education (CPE) hours per year for a total of 30 hours over each three-year re-qualification period. CPE hours must be reported to PCI SSC at the end of each year prior to the qualification anniversary date. Approved methods for obtaining and reporting CPE credit are documented in the *CPE Maintenance Guide*. The requirement to:
 - begin collecting CPE hours becomes effective January 1, 2015;
 - reporting of CPE hours becomes effective September 1, 2015.

3 PCIP Course Description

The PCIP training comprises an online course providing an overview of PCI Standards and information regarding:

- The different PCI Standards, including PCI DSS, PA-DSS, PTS and P2PE
- Payment Card Industry (PCI) terminology, roles and transaction flow
- PCIP Professional ethical requirements under the PCI Code of Professional Responsibility
- Cardholder data and applicability of the PCI DSS
- The intent of PCI DSS requirements
- When and how Self-Assessment Questionnaires (SAQs) are used
- The location and use of the various PCI SSC Information Supplements
- How new technologies such as P2PE, tokenization, mobile devices, and cloud computing can affect PCI compliance
- Appropriate uses of compensating controls
- How to apply PCI DSS requirements to a given case study

4 Credential Policies

4.1 Use of the Credential

While PCIP qualification is active, PCIPs may use the credential “PCIP” and the PCIP logo after their names. In addition, a searchable, online list of PCIPs will be posted and available to the public on the PCI SSC Website (the “List of PCIPs”).

Please note that PCIP qualification does not confer rights and privileges associated with other PCI SSC qualifications.

4.2 Grace Period for Lapsed Qualifications and Credentials

Individuals are given a 14-day grace period following their PCIP qualification expiration date to meet the maintenance requirements, and thereby renew their PCIP qualification. However, names of individuals with lapsed qualifications will be removed from the List of PCIPs as of the day following the expiration date.

The renewal date of a successfully renewed qualification will be the date three years after the expiration date of the last PCIP qualification. Qualifications that have expired for more than 14 days cannot be renewed by satisfying maintenance requirements. Individuals wishing to renew more than 14 days after their qualification has lapsed must reapply as new PCIP candidates.

4.3 Exam Security

The PCIP qualification exam and all exam-related materials are the sole and exclusive property of PCI SSC. Individuals taking the PCIP exam are required to keep these materials confidential and not to make them available to any person or entity for any reason.

Maintaining the security of the PCIP examination is essential to uphold the integrity of the qualification program. Conduct that violates the security of PCIP examinations and PCIP program policy includes, but is not limited to:

- Theft of any PCI SSC examination or portion thereof
- Recording PCI SSC examination content in any format
- Unauthorized access to any PCI SSC exam
- Reproducing or reconstructing PCI SSC examination material without authorization
- Using improperly obtained PCI SSC test questions to prepare persons for PCI SSC examination
- Impersonating an examinee or using an impersonator to take any PCI SSC examination
- Using prohibited or unauthorized materials, notes, or computer programs during any PCI SSC exam
- Providing or communicating unauthorized information to (or otherwise aiding) another person during any PCI SSC exam
- Any other breach of PCI SSC examination security

A breach in examination security has significant repercussions for PCI SSC, including but not limited to, the costs of replacing questions and developing new exams. Individuals who violate exam security may be disqualified from the exam, as well as future exams administered by or on behalf of PCI SSC. PCI SSC reserves the right to pursue any and all legal, equitable, and/or other remedies against any individual who breaches the security of any such exam, including without

limitation, revocation of any or all PCI SSC qualifications and/or damages for costs associated with replacing compromised exam questions and developing new exams.

4.4 Practitioner Feedback

Practitioner feedback can be provided regarding an active PCIP from a colleague or an entity to which the PCIP provides services or support. Feedback must be submitted using the online *PCIP Feedback Form* located on the PCI SSC Website. Feedback must include the name of the PCIP and a detailed description of the comments or observations.

4.5 Suspension and Revocation

When PCI SSC has reason to believe that accusations against an active PCIP may be valid, it will investigate and notify the PCIP. The PCIP will have the opportunity to present his or her defense to PCI SSC according to the terms outlined in the *Appeals Policy* section below.

PCI SSC may, at its sole discretion, take disciplinary action (such as issuing a warning or suspending or revoking an individual's status as a PCIP) for cause. Cause for such disciplinary action (each a "Violation") includes, but is not limited to:

- Failure to comply with the terms of the Code or any agreement with PCI SSC
- Fraud or submission of inaccurate application or qualification data to obtain or maintain PCIP status
- Any conduct prohibited by (or otherwise contrary to) the requirements of any PCI SSC program in which the PCIP is a participant, including but not limited to the requirements set forth in the Exam Security section above
- Failure to provide proof of Continuing Professional Education (CPE) hours

4.6 Appeals Policy

An appeals procedure is available to any individual who has obtained or applied for PCIP status and wishes to appeal an adverse decision affecting his or her PCIP status.

A request for review and consideration must be submitted in writing via a traceable mail service to the PCIP Program Manager no more than 30 days from the date of notification of the adverse decision notice by PCI SSC. The request must state the reasons why the decision is being contested and include supporting evidence or documentation in support of the appeal. Any individual who does not file a request for an appeal within the required time limit and in accordance with applicable program procedures waives the right to appeal.

PCI SSC will review all relevant evidence submitted and provide a written response to the candidate within 60 days of receiving the appeal request. For all appeals, PCI SSC may decide to uphold the initial decision or may take other appropriate action. PCI SSC is the final authority for all qualification and disciplinary action appeals, and all decisions made by PCI SSC in connection therewith are final and binding on the individual requesting the appeal. The foregoing appeal right is exclusive and sets forth the sole remedy and PCI SSC's sole obligation to a PCIP or candidate in connection with the corresponding disciplinary action or appeal.

4.7 Privacy Policy

PCIP applications and exam results are confidential, except that the names of those achieving PCIP status are searchable in the List of PCIPs. Names of those who do not pass the exam are not disclosed by PCI SSC. PCI SSC will release individual application and pass/fail results only to the corresponding candidate.

Appendix A: PCIP Application

PCI SSC Payment Card Industry Professional Qualification Application

Complete all sections fully and accurately

All applications must be completed online via the PCI SSC website

Section I. Identification and Contact Information

Please provide the address you would like PCI SSC to use for all correspondence.

Name:	First:		Middle initial:		Last:	
Address:						
City:				State/Province:		
Country:				Postal Code:		
Daytime telephone:				E-mail:		

Section II: Qualifications

Please indicate any other PCI SSC qualifications that you currently hold.

<input type="checkbox"/>	QSA	<input type="checkbox"/>	ISA	<input type="checkbox"/>	PA-QSA	<input type="checkbox"/>	Other:	
--------------------------	-----	--------------------------	-----	--------------------------	--------	--------------------------	--------	--

Please indicate any other PCI SSC qualifications that you have held in the past.

<input type="checkbox"/>	QSA	<input type="checkbox"/>	ISA	<input type="checkbox"/>	PA-QSA	<input type="checkbox"/>	Other:	
--------------------------	-----	--------------------------	-----	--------------------------	--------	--------------------------	--------	--

Please indicate any security or audit qualifications that you currently hold.

<input type="checkbox"/>	CISA	<input type="checkbox"/>	CISM	<input type="checkbox"/>	CISSP	<input type="checkbox"/>	Other:	
--------------------------	------	--------------------------	------	--------------------------	-------	--------------------------	--------	--

Section III: Employment

Number of years of experience in the payments security industry:

<input type="checkbox"/>	Less than 1 year	<input type="checkbox"/>	1 to 2 years	<input type="checkbox"/>	3 to 5 years	<input type="checkbox"/>	More than 5 years
<input type="checkbox"/>	Please confirm an up-to-date copy of your resume or CV is included with your application.						

Please list your employers for the past two years, beginning with the most recent.

Section III: Employment *(continued)*

Employer #1 *Your current or most recent position. If you are not currently employed, please include the end date for your most recent position held.*

Job title:		Start date:	mm/yy	End Date:	mm/yy
------------	--	-------------	-------	-----------	-------

Applicable duties and responsibilities:

Company name:					
Telephone:		Supervisor's E-mail:			
Address:		City:			
State/Province:		Country:		Postal Code:	

Employer #2

Job title:		Start date:	mm/yy	End Date:	mm/yy
------------	--	-------------	-------	-----------	-------

Applicable duties and responsibilities:

Company name:					
Telephone:					
Address:		City:			
State/Province:		Country:		Postal Code:	

Employer #3

Job title:		Start date:	mm/yy	End Date:	mm/yy
------------	--	-------------	-------	-----------	-------

Applicable duties and responsibilities:

Company name:					
Telephone:					
Address:		City:			
State/Province:		Country:		Postal Code:	

Section IV: Payment of Fees

All PCIP Program Fees are nonrefundable. Please contact PCI SSC if you have questions regarding your eligibility for qualification prior to submitting your application.

Each PCIP applicant must provide the required fee to PCI SSC in advance of PCI SSC reviewing the application. This fee may be paid by check or other means approved by PCI SSC. All checks should be made payable to "PCI SSC" and mailed to PCI SSC at the following address:

PCI Security Standards Council
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone number: (781) 876-8855

Note:

All fees are subject to change and are non-refundable.

Section V: Application Attestation

By signing this application below, I hereby acknowledge, certify to PCI SSC and agree that:

- (a) I am the above-named applicant;
- (b) all statements made and information contained in this application or that I otherwise provide to PCI SSC are and will be true and correct to the best of my knowledge and belief at the time;
- (c) if I register for any PCIP training or qualification examination I will do so under my own name and no others;
- (d) if I receive any PCI SSC qualification under false circumstances, I will immediately surrender any corresponding qualification credentials to PCI SSC;
- (e) I will provide to PCI SSC any requested documentation in connection with this application and my status as a PCIP;
- (f) PCI SSC may contact current and previous employers listed in this application to verify my employment status;
- (g) I have read and understand the *PCIP Qualification Requirements* and the *Code of Professional Responsibility* attached as Appendix B thereto (the “Code”), and at all times while I am either a PCIP or PCIP candidate I will advocate, adhere to, and support the Code, and comply with all PCI SSC policies and requirements outlined therein or otherwise established by PCI SSC from time to time for PCIPs;
- (h) if I am qualified as a PCIP, PCI SSC may list my name, contact information and qualification, suspension and/or revocation status on the List of PCIPs;
- (i) I will use the PCIP designation only as permitted by PCI SSC policies and only while my PCIP qualification remains in effect;
- (j) all exams and exam questions administered in connection with the PCIP Program and/or other PCI SSC programs are confidential and, unless required by law, I will not (i) record, copy or retain any such test or test questions, (ii) reproduce, transmit or otherwise disclose or provide access to any of the foregoing in any form to any other person or organization (other than PCI SSC and its agents) or (iii) otherwise aid any other person during any such exam;
- (k) I will not engage in, and I have not within the past 24 months engaged in, any of the following conduct:
 - (i) violated any requirement regarding nondisclosure of confidential materials; (ii) failed to maintain physical, electronic or procedural safeguards to protect confidential or sensitive information as required; (iii) failed to report unauthorized access to any system storing confidential or sensitive information; (iv) engaged in any criminal or unprofessional or unethical business conduct; (v) cheated on any exam in connection with any PCI SSC program or qualification; (vi) failed to comply with any requirement of any qualification issued to me by PCI SSC; or (vii) failed to promptly notify PCI SSC of any event described above that occurs after the date hereof; and
- (l) each qualification and/or credential granted or issued to me by PCI SSC in connection with any PCI SSC program is subject to (i) required re-qualification and (ii) immediate suspension and/or revocation if PCI SSC determines, in its sole discretion, that I have failed to comply with, satisfy or adhere to any of the foregoing.

Section V: Application Attestation *(continued)*

Additionally, I hereby waive all claims and agree to indemnify and hold harmless PCI SSC for any action taken pursuant to the rules and standards of PCI SSC with regard to my PCIP application, PCIP examination(s) and/or my PCIP status, except claims based on the gross negligence or willful misconduct of PCI SSC.

Signature ↑	Date ↑

Appendix B: Code of Professional Responsibility

The PCI Security Standards Council (PCI SSC) is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. PCI SSC's mission is to enhance payment account data security by driving education and awareness of the PCI SSC security standards (the "PCI Standards"). To help achieve this goal, PCI has adopted this Code of Professional Responsibility to help ensure information security professionals adhere to the highest standards of ethical and professional conduct. Adherence with this Code will help ensure the safe handling of cardholder information and enhance payment card data security.

All PCI SSC-qualified individuals and all PCI SSC qualification candidates must advocate, adhere to, and support the following Code of Professional Responsibility. PCI SSC-qualified individuals who intentionally or knowingly violate any principle of this Code will be subject to revocation of qualification and/or other disciplinary action by PCI SSC.

Principles

Professional Competence and Due Care

- Perform each aspect of your work honorably, responsibly, and legally
- Act in the best interests of all entities that you provide services or support to, while maintaining high standards of conduct and being consistent with the PCI Standards and guidance
- Deliver diligent and competent services in accordance with the PCI Standards and applicable laws
- Render only those services for which you are fully competent and qualified
- Promptly advise all entities that you provide services or support to on changes in PCI Standards and guidance
- Participate in learning throughout your career to maintain the knowledge, skills and expertise needed in the payment security industry
- Promote current information security best practices and standards

Security and Confidentiality

- Respect and safeguard confidential, proprietary, or otherwise sensitive information with which you come into contact in the course of professional activities, unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties
- Take affirmative steps to comply with the PCI Standards to assure that confidential information is maintained securely
- Immediately notify the appropriate authorities and proper industry personnel should you suspect a compromise or breach in security

Integrity

- Refrain from conduct which would damage or reflect poorly on the reputation of PCI SSC, its standards, the profession, or the practice of colleagues, clients, and employers
- Report ethical violations to PCI SSC in a timely manner
- Refrain from any activities which might constitute a conflict of interest
- Perform all duties with objectivity

Compliance with Industry Laws and Standards

- Perform duties in accordance with the PCI Standards
- Comply with existing laws and regulations, with local laws taking precedence over PCI Standards
- Co-operate with law enforcement agencies

Violation and Enforcement

Depending on the severity of the Violation, disciplinary action could include:

- Warning: A written warning could be issued that specifies the consequences if the situation occurs again, or if there is another Violation.
- Suspension: PCI SSC qualification could be suspended for all programs in which the individual participates.
- Revocation: PCI SSC qualification could be revoked for all programs in which the individual actively participates.

PCI SSC is committed to enforcing its Code of Professional Responsibility, and has adopted a procedure that allows fair and objective review of allegations of violations of the Code.