



Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire A and Attestation of Compliance

**All cardholder data functions outsourced. No
Electronic Storage, Processing, or Transmission
of Cardholder Data**

Version 2.0

October 2010

Document Changes

Date	Version	Description
October 1, 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 28, 2010	2.0	To align content with new PCI DSS v2.0 requirements and testing procedures.

Table of Contents

Document Changes	i
PCI Data Security Standard: Related Documents	ii
Before you Begin	iii
Completing the Self-Assessment Questionnaire	iii
PCI DSS Compliance – Completion Steps	iii
Guidance for Non-Applicability of Certain, Specific Requirements	iii
Attestation of Compliance, SAQ A	1
Self-Assessment Questionnaire A.....	4
Implement Strong Access Control Measures	4
Requirement 9: Restrict physical access to cardholder data.....	4
Maintain an Information Security Policy	5
Requirement 12: Maintain a policy that addresses information security for all personnel.....	5
Appendix A: (not used).....	6
Appendix B: Compensating Controls	7
Appendix C: Compensating Controls Worksheet	8
Compensating Controls Worksheet – Completed Example.....	9
Appendix D: Explanation of Non-Applicability	10

PCI Data Security Standard: Related Documents

The following documents were created to assist merchants and service providers in understanding the PCI Data Security Standard and the PCI DSS SAQ.

Document	Audience
<i>PCI Data Security Standard: Requirements and Security Assessment Procedures</i>	All merchants and service providers
<i>Navigating PCI DSS: Understanding the Intent of the Requirements</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Guidelines and Instructions</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C-VT and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Eligible merchants and service providers ¹
<i>PCI Data Security Standard and Payment Application Data Security Standard: Glossary of Terms, Abbreviations, and Acronyms</i>	All merchants and service providers

¹ To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Guidelines and Instructions*, "Selecting the SAQ and Attestation That Best Apply to Your Organization."

Before you Begin

Completing the Self-Assessment Questionnaire

SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their systems or premises.

SAQ A merchants, defined here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their systems or premises. Such merchants validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your systems or premises, but relies entirely on third party service provider(s) to handle all these functions;
- Your company has confirmed that the third party(s) handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

This option would never apply to merchants with a face-to-face POS environment.

Each section of the questionnaire focuses on a specific area of security, based on the requirements in the *PCI DSS Requirements and Security Assessment Procedures*. This shortened version of the SAQ includes questions which apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment which are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

PCI DSS Compliance – Completion Steps

1. Assess your environment for compliance with the PCI DSS.
2. Complete the Self-Assessment Questionnaire (SAQ A) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
3. Complete the Attestation of Compliance in its entirety.
4. Submit the SAQ and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

Guidance for Non-Applicability of Certain, Specific Requirements

Non-Applicability: Requirements deemed not applicable to your environment must be indicated with "N/A" in the "Special" column of the SAQ. Accordingly, complete the "Explanation of Non-Applicability" worksheet in Appendix D for each "N/A" entry.

Attestation of Compliance, SAQ A

Instructions for Submission

The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at "PCI DSS Compliance – Completion Steps" in this document.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	ZettaGrid Pty Ltd	DBA(S):	ZettaGrid
Contact Name:	Nicholas Power	Title:	General Manager
Telephone:	+61 8 6314 6580	E-mail:	nicholas.power@zettaGrid.com
Business Address:	Level 6, 10 William Street	City:	Perth
State/Province:	WA	Country:	Australia
		ZIP:	6000
URL:	www.zettaGrid.com		

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

Company Name:	Vectra Corporation Ltd		
Lead QSA Contact Name:	Kelvin Heath	Title:	Chief Security Officer
Telephone:	(02) 9276 1886	E-mail:	kelvin.heath@vectra-corp.com
Business Address:	504 / 3 Spring St.	City:	Sydney
State/Province:	NSW	Country:	Australia
		ZIP:	2000
URL:	www.vectra-corp.com		

Part 2. Type of merchant business (check all that apply):

☐ Retailer
 ☐ Telecommunication
 ☐ Grocery and Supermarkets
☐ Petroleum
☒ E-Commerce
☒ Mail/Telephone-Order
☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Head Office: Level 6, 10 William Street, Perth WA.

Sales Office: Level 7, 157 Walker Street, North Sydney, NSW.

Part 2a. Relationships

Does your company have a relationship with one or more third-party agents (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? ☐ Yes ☒ No

Does your company have a relationship with more than one acquirer? ☐ Yes ☒ No

Part 2b. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- ☒ Merchant does not store, process, or transmit any cardholder data on merchant systems or premises but relies entirely on third party service provider(s) to handle these functions;
- ☒ The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant;
- ☒ Merchant does not store any cardholder data in electronic format; **and**
- ☒ If Merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically.

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated 28th October 2014, Zettagrid asserts the following compliance status (check one):

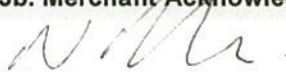
- ☒ **Compliant:** All sections of the PCI SAQ are complete, and all questions answered "yes," resulting in an overall **COMPLIANT** rating, thereby Zettagrid has demonstrated full compliance with the PCI DSS.
- ☐ **Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered "no," resulting in an overall **NON-COMPLIANT** rating, thereby (Merchant Company Name) has not demonstrated full compliance with the PCI DSS.
 - **Target Date** for Compliance:
 - An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.

Part 3a. Confirmation of Compliant Status

Merchant confirms:

- ☒ PCI DSS Self-Assessment Questionnaire A, Version 2.0, was completed according to the instructions therein.
- ☒ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment.
- ☒ I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.

Part 3b. Merchant Acknowledgement


Signature of Merchant Executive Officer ↑

Nicholas Power

Merchant Executive Officer Name ↑

Zettagrid Pty Ltd

Merchant Company Represented ↑

28/10/2014
Date ↑

General Manager

Title ↑

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (If Compliance Status is "NO")
		YES	NO	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Self-Assessment Questionnaire A

Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.

Date of Completion: 28th October 2014

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response:	Yes	No	Special*
9.6	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls include the following:				
9.7.1	Is media classified so the sensitivity of the data can be determined?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.8	Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media (especially when media is distributed to individuals)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9	Is strict control maintained over the storage and accessibility of media?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.10	Is all media destroyed when it is no longer needed for business or legal reasons?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Is destruction performed as follows:				
9.10.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are containers that store information to be destroyed secured to prevent access to the contents? (For example, a "to-be-shredded" container has a lock preventing access to its contents.)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Question		Response:		
		Yes	No	Special*
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, as follows?			
12.8.1	Is a list of service providers maintained?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.