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

PCI Data Security Standard: Related Documents

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

Document	Audience
PCI Data Security Standard: *Requirements and Security Assessment Procedures*	All merchants and service providers
Navigating PCI DSS: *Understanding the Intent of the Requirements*	All merchants and service providers
PCI Data Security Standard: *Self-Assessment Guidelines and Instructions*	All merchants and service providers
PCI Data Security Standard: *Self-Assessment Questionnaire A and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire B and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire C-VT and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire C and Attestation*	Eligible merchants[1]
PCI Data Security Standard: *Self-Assessment Questionnaire D and Attestation*	Eligible merchants and service providers[1]
PCI Data Security Standard and Payment Application Data Security Standard: *Glossary of Terms, Abbreviations, and Acronyms*	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 B) 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:	Wikimedia UK	DBA(s):			
Contact Name:	Mr. Richard Symonds	Title:	Office Manager		
Telephone:	02070650991	E-mail:	paypal@wikimedia.org.uk		
Business Address:	56-64 Leonard Street	City:	London		
State/Province:	Non-USA	Country:	United Kingdom	ZIP:	EC2A 4L
URL:	www.wikimedia.org.uk				

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

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		Zip:	
URL:					

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

☐Retailer ☐Telecommunication ☐Grocery and Supermarkets

☐Petroleum ☐E-Commerce ☐Mail/Telephone-Order ☒Others (please specify):

Charity

List facilities and locations included in PCI DSS review:

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 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 B dated 09/20/2012 , Wikimedia UK 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 Wikimedia UK has demonstrated full compliance with the PCI DSS.

☐ **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or some questions are answered "no," resulting in an overall **NON-COMPLIANT** rating, thereby Wikimedia UK 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 in all material respects.
☒	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.

Part 3b. Merchant Acknowledgement

Richard Symonds (electronically signed, in secure authenticated session)	09/20/2012
Signature of Merchant Executive Officer ↑	*Date ↑*
Richard Symonds	Office and Development Manager
Merchant Executive Officer Name ↑	*Title ↑*
Wikimedia UK	
Merchant Company Represented ↑	

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	☒	□	
12	Maintain a policy that addresses information security	☒	□	

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: 09/20/2012

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)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	□	□	N/A
9.7		(a) Is strict control maintained over the internal or external distribution of any kind of media?	□	□	N/A
		(b) Do controls include the following:			
	9.7.1	Is media classified so the sensitivity of the data can be determined?	□	□	N/A
	9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	□	□	N/A
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)?	□	□	N/A
9.9		Is strict control maintained over the storage and accessibility of media?	□	□	N/A
9.10		Is all media destroyed when it is no longer needed for business or legal reasons?	□	□	N/A
		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?	□	□	N/A
		(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.)	□	□	N/A

* "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 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?		☒	□	
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?		☒	□	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?		☒	□	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?		☒	□	

[*] "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.

Appendix A: (not used)

This page intentionally left blank

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

   Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if; (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES" was checked and compensating controls were mentioned in the "Special" column.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	**Explanation**
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet—Completed Example

Use this worksheet to define compensating controls for any requirement where "YES" was checked and compensating controls were mentioned in the "Special" column.

Requirement Number: *8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the SU-log directory. In this way, each user's actions can be tracked through the SU account.*
7. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges*
8. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged*

Appendix D: Explanation of Non-Applicability

If "N/A" or "Not Applicable" was entered in the "Special" column, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example: *9.3.1*	*Visitors are not allowed in areas where cardholder data is processed or maintained.*
Please see Appendix E for explanations of all answers, including all answers of "Non-Applicable".	

Appendix E: Justification for All Answers

The following table gives additional information and justification (where appropriate) for the answers recorded above.

Question	Justification of Answer
9.6	This question's text is "Are all paper records or other hardcopy materials that contain cardholder data physically secure?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.7.a	This question's text is "Is strict control maintained over the internal or external distribution of paper records that contain cardholder data?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.7.1	This question's text is "Do your distribution controls require that paper records containing cardholder data are always classified so they can be identified as confidential?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": The question of whether we maintain strict control over the internal or external distribution of any kind of media (paper or electronic) that contains cardholder data does not apply to us. We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.7.2	This question's text is "Do your distribution controls require that paper records containing cardholder data can be sent only by secured courier or other delivery method that can be accurately tracked?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": The question of whether we maintain strict control over the internal or external distribution of any kind of media (paper or electronic) that contains cardholder data does not apply to us. We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]

9.8	This question's text is "Are processes and procedures in place to ensure that logs are maintained to track all paper records or hardcopy materials containing cardholder data that is moved from a secured area, and that management approval is obtained prior to moving any and all paper records or hardcopy materials containing cardholder data from a secured area (especially when media is distributed to individuals)?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.9	This question's text is "Is strict control maintained over the storage and accessibility of paper records that contain cardholder data?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.10	This question's text is "Are paper records containing cardholder data destroyed when they are no longer needed for business or legal reasons?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.10.1.a	This question's text is "When destroying unneeded records containing cardholder data, are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": The question of whether we destroy media containing cardholder data when it is no longer needed does not apply to us. We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]
9.10.1.b	This question's text is "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)?". This question's answer is "Not Applicable". Following is a collection of determinations that we have made leading us to conclude that the answer is "Not Applicable": The question of whether hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed does not apply to us. The question of whether we destroy media containing cardholder data when it is no longer needed does not apply to us. We NEVER have PANs (or any other sensitive cardholder data) recorded on paper. [Tracking: Our answer was "No" to the question "Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?"]

12.8	This question's text is "Do you have and enforce policies and procedures to manage service providers with whom you share cardholder data?". This question's answer is "Yes". Following is a collection of determinations that we have made leading us to conclude that the answer is "Yes": We have taken this remedial action: "Follow all instructions to put your new information security policy into effect." (This question passed in part because the following sub-question(s) passed: 12.8.1, 12.8.2, 12.8.3, 12.8.4)
12.8.1	This question's text is "Do you maintain a list of service providers?". This question's answer is "Yes". Following is a collection of determinations that we have made leading us to conclude that the answer is "Yes": We have taken this remedial action: "Follow all instructions to put your new information security policy into effect."
12.8.2	This question's text is "Do you maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess?". This question's answer is "Yes". Following is a collection of determinations that we have made leading us to conclude that the answer is "Yes": We have taken this remedial action: "Follow all instructions to put your new information security policy into effect."
12.8.3	This question's text is "Have you established a process for engaging service providers, including proper due diligence prior to engagement?". This question's answer is "Yes". Following is a collection of determinations that we have made leading us to conclude that the answer is "Yes": We have taken this remedial action: "Follow all instructions to put your new information security policy into effect."
12.8.4	This question's text is "Do you maintain a program to monitor service providers' PCI DSS compliance status?". This question's answer is "Yes". Following is a collection of determinations that we have made leading us to conclude that the answer is "Yes": We have taken this remedial action: "Follow all instructions to put your new information security policy into effect."

Appendix F: Text of Questions Asked and Answers Given

The following table gives the text of the questions asked of us and the answers we gave to them, from which the answers recorded above in the SAQ were derived.

Question Asked	Answer Given
Do you process payments using a POS terminal, a Virtual Terminal, other Payment Application, and/or an Imprint Machine ("knuckle-buster")?	No
Do you see customers face-to-face who pay you using their payment cards?	No
Do you rely ENTIRELY on one or more third-party service providers (i.e. payment gateways, hosting providers) to handle ALL processing, storing, and/or transmitting of cardholder data for you?	Yes
Is it your policy or practice to use physical security measures to protect your facilities and any sensitive data or equipment that you have there?	Yes
Do you (even occasionally or temporarily) create, receive, or otherwise come to possess any paper records or receipts that contain cardholder data?	No
(PCI DSS Requirement 12.8) - Do you have and enforce policies and procedures to manage service providers with whom you share cardholder data?	Yes
(PCI DSS Requirement 12.8.1) - Do you maintain a list of service providers?	Yes
(PCI DSS Requirement 12.8.2) - Do you maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess?	Yes
(PCI DSS Requirement 12.8.3) - Have you established a process for engaging service providers, including proper due diligence prior to engagement?	Yes
(PCI DSS Requirement 12.8.4) - Do you maintain a program to monitor service providers' PCI DSS compliance status?	Yes

Appendix G: Remediation Plan

The following table gives the plan for remediating the PCI DSS requirements that were not met on our first pass through the SAQ.

Label	Remedial Action	Dependencies	Dates
Get ExpertPCI Security Policy	Get the ExpertPCI PCI-Compliant Security policy.		Done: 20-Sep-2012
Get ExpertPCI Incident Response Plan	Get the ExpertPCI PCI-Compliant incident response plan.		Done: 20-Sep-2012
Follow Security Policy Instructions	Follow all instructions to put your new information security policy into effect.		Done: 20-Sep-2012