Payment Card Information Self-Assessment Questionnaire Checklist

Due: November 9

Schedule an initial consultation appointment with the Payment Card Coordinator, Contact: merchantservices@ucsc.edu

Click each item to download a general template. Templates for these items can also be found on the Merchant Services webpage. Full descriptions of each item on this list can be found on pages two and three of this document. Update, or prepare the following required documentation:

☐ Departmental Credit Card Security Policy

- E-Commerce (for SAQ A environments)
- Card-Present (for SAQ B or SAQ P2PE environments)

Note: If you use Card-Present *and* E-Commerce, combine SAQ A with SAQ B or SAQ P2PE.

☐ Incident Response Plan

☐ Training & Policy Certification

☐ Service Provider List

☐ Access control list

☐ Vendor Responsibility Matrix (SAQ A Template, SAQ B Template, SAQ P2PE Template)

☐ Contract information and AOC for Credit Card processor and involved third parties:

- E.g. Payment processor (Freedompay, Auth.net), Integration software (Ecwid, etc.)
- Attestation of Compliance (AOC) from payment processor and/or website host

☐ Complete SAQ(s) in VigiOne Portal

E-Commerce Only Document	
☐ Attestation of E-Commerce Only Processing	E-Commerce *only* merchants with no Card-Present environment
Card-Present Environment Documents	
☐ Equipment Tracking List ☐ Terminal Tamper Inspection Checklist ☐ Photos of Credit Card Terminals: • Front and back, clearly capturing serial number information • Can be kept in a word document or as individual files	These documents apply to *Card-Present Merchants only* (SAQ B or SAQ P2PE). If you only perform E-Commerce, use the Attestation of E-Commerce Only Processing form above instead of these.

Payment Card Information Self-Assessment Questionnaire Checklist

Due: November 9

Document Descriptions:

Departmental Credit Card Security Policy: This document outlines the policies and procedures put into place by your department to protect cardholder data. This is often one of the more time consuming aspects of establishing your PCI compliance documentation, so plan ahead and give yourself time to complete it. Not all aspects of the template may apply to your current operation. You are welcome to delete sections that do not apply to your organization. Versions are available for Card-Present *and* E-commerce only. If your department does both, combine these two documents. If you are not comfortable doing so, please contact merchantservices@ucsc.edu.

Incident Response Plan: This document prepares your unit for efficient action and communication in the event of a suspected or confirmed breach of a physical, or digital environment. Most critically, it should contain the exact steps of what to do under breach circumstances, as well as contact information of the person in the unit/division that will report the breach to relevant parties. Typically this is the PCI Coordinator for the unit reporting to the Payment Card Coordinator by phone and by emailing merchantservices@ucsc.edu.

Training & Policy Certification: This document is signed by the departmental PCI Coordinator and Department Head to certify that they understand that critical aspects of UCSC's PCI and Merchant policies and procedures are to be followed. Full details are available in the document.

Service Provider List: This document lists all service providers, including a description of service provided. Depending on the complexity of your environment, this could be as few as one service provider or more than three. Generally our acquiring bank is not listed (Bank of America). Please list contact information for each party so that they can be reached in the event of a breach or other emergency.

Access Control List: Documentation of anyone that has access to your credit card environment and their access level. This list enables your organization to know who should and should not be involved with credit card processing and management environments so that if unusual activity occurs you know who is cleared to be involved and who isn't.

Vendor Responsibility Matrix: This matrix assigns specific security control requirements to both you (the merchant) and service providers (any third-party involved in processing, storing, or transmitting cardholder data). Request this document from your third party service providers. If they do not provide one, please send them the appropriate template and have them fill it out. If you need assistance obtaining a completed Vendor Responsibility Matrix, please contact merchantservices@ucsc.edu.

Contract information for your Credit Card Vendor and/or Service Providers: All parties engaging in business with UCSC should be contracted, and contracts with companies dealing with Card Data must be on file in order for UCSC to ensure that the third party is compliant with PCI DSS regulations. If a party is in-scope of PCI (Freedompay, Authorize.net, web hosts with payment redirects, etc.) an up-to-date QSA signed AOC must also be on file. These parties must also agree to UC's Security Appendix DS. You can

request this information from your Service Providers, Procurement, or ask merchantservices@ucsc.edu for assistance in obtaining contract information.

Equipment Tracking, Photos and Movement List: List of all credit card terminals, models, serial numbers, their physical locations, and pictures of each terminal, front and back. This information is critical to provide baseline information for tamper checks and equipment tracking. Depending on the number of terminals and frequency of their movement, different tracking sheets and methods can be used. Tracking of terminal movement and logging of employees moving them deters improper access and creates an access log for audit in the event of a breach or audit.

Terminal Tamper Inspection Log: Proof that terminals are being inspected on a regular basis.

Attestation of Ecommerce only Processing: For E-commerce only merchants, a statement attesting that no physical credit card terminals are being used can be submitted instead of a tracking list. This statement should be signed by the departmental PCI Coordinator and Department Head.

When is my SAQ Due?
SAQ's must be submitted with attached supporting evidence by **November 9**.

How do I get help?
If you need assistance with any aspects of your SAQ please email merchantservices@ucsc.edu.

Where do I complete my SAQ?
SAQ's can be completed on the VigiOne website. Please click the link on page one to access this website.