Office of the Controller
Accounting and Reporting Services
Merchant Services

MERCHANT SERVICES AND PCI DSS COMPLIANCE MANUAL

Merchant Account Guidelines and Procedures

Created by: Katherine Cochran, October 24, 2016
Last revision by: Katherine Cochran, May 20, 2024
Approved by: Edgar Salazar, May 24,2024

Table of Contents

Overview

Florida International University (FIU) must meet specific annual reporting requirements to ensure the University is complying with all the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

The Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing cardholder data security, intended to help organizations proactively protect cardholder data, which was developed by the founding payment brands of the Payment Card Industry Security Standards Council. All merchants and service providers are required to comply with PCI DSS. Cardholder data is of high value to malicious individuals because the information can be used to generate factious payment cards and process fraudulent transactions. A merchant must ensure that appropriate safeguarding measures are in place to protect cardholder data. Merchants validate their PCI compliance via a Self-Assessment Questionnaire (SAQ).

The Controller's Office and the Division of Information Technology have joined efforts to meet PCI reporting requirements. The area of Merchant Services in the Controller's Office serves as the liaison between the department and our acquiring bank, and as a primary contact regarding any merchant reporting requirements. The SAQ submission can only be executed if each merchant location completes their assigned questionnaire. Lack of compliance in a single area of the University could jeopardize the University's ability as a whole to accept payment cards. Therefore, this is an on-going effort, and each department must work together to ensure that FIU is continuously in compliance. Failure to comply with the PCI DSS may result in significant fines, legal liability, reputation damage and loss of business for the University.

Purpose and Scope

To establish a formal process that will educate the FIU community and ensure that all merchant locations are adhering to the University's policies and procedures while maintaining compliance with PCI requirements. The Merchant Services and PCI DSS Compliance Manual clarifies roles and responsibilities for the employees involved and provides guidance for potential merchant locations.

Approved Methods of Payment Card Processing

Card Present Transactions

- **Stand-Alone Terminal** - Device procured through FIU's preferred validated point-to-point encryption (P2PE) solution vendor, Bluefin Payment Solutions, or device procured through our acquiring bank that is connected via an analog line for dial-up connection or wireless via a cellular carrier.
- **Mobile Payments** – Device procured through FIU's preferred validated P2PE solution vendor, Bluefin Payment Solutions or department purchased iPads that connect to a cellular carrier that are deemed a sole-purpose workstation (additional security software will be installed to make the iPads compliant).
- **Point of Sale** – Device and software must be approved by the PCI Compliance Team.

Card-Not Present Transactions

- **Mail-Order-Telephone Order (MOTO)** – Device procured through FIU's preferred validated point-to-point encryption (P2PE) solution vendor, Bluefin Payment Solutions.
- **E-Commerce**- Internet payment card application recommended by FIU's PCI Compliance Team and implemented through the Division of Information Technology Enterprise Web Services.
- **Fully Outsourced to a PCI Compliant Vendor**- The vendor must be listed on Visa's Global Registry of Service Providers and provide an Attestation of Compliance (AOC) that meets the latest version of PCI DSS and all other supporting compliance documentation as deemed necessary by the PCI Compliance Team.

The University has a master agreement with Eventbrite, a merchant services provider that offers an online platform to accept credit card payments for event ticket sales, conference/webinar registration fees, etc. The Controller's Office is centrally managing all account set-up and users access for departments interested in using Eventbrite. For all related inquiries, please contact Merchant Services via email at merchant@fiu.edu.

Any exceptions to the methods mentioned above must be evaluated and approved by the PCI Compliance Team. Email your exception request to pcicompliance@fiu.edu with a detailed justification of why an exception is needed for the team's evaluation and approval.

Business Unit Requirements

On-Boarding Process for a Merchant Account

The following requirements are intended for departments and units interested in applying for a merchant ID number and for existing merchant locations that are changing their merchant process:

- Complete and submit a Merchant Application.
- Establish/Update your department's Merchant Procedures
- Delegate a Business and an IT contact (responsible for the department's overall merchant environment).
- Complete the assigned annual Self-Assessment Questionnaire (SAQ).
- Submit/Manage a list of your merchant employees to Merchant Services as requested.
- Employees shall not use vendor-supplied defaults for system passwords. Also, group, shared, or generic accounts and passwords are prohibited.
- Approval must be obtained from Merchant Services and the PCI Compliance Team to process credit card payments and/or before entering into any contracts or purchases of software and/or equipment related to credit card processing.
- Merchants must notify Merchant Services and the PCI Compliance Team of software upgrades and personnel changes related to credit card processing.

Additional requirements specific to online payment processing:

- Submit initial/updated privacy and refund policy to the Office of General Counsel for approval and subsequently list both on your FIU webpage along with a dedicated customer service number.

- Prepare required third party vendor documentation to submit the agreement via the Total Contract Management (TCM) tool:
    - Submit the Attestation of Compliance (AOC) for Third Party Service Providers (TPSP)
    - Submit latest vulnerability scan report, if applicable
    - Submit Schematic- a data flow diagram that clearly defines the systems and vendors (gateway, processor, etc.) involved in the exchange of the cardholder data flow.
    - Submit a PCI Responsibility Matrix (applicable if FIU is the Merchant of Record (owns the merchant ID) if deemed necessary by the PCI Compliance team.

The merchant location's business contact and designated back-up are responsible for ensuring all employees who will be involved in payment card processing or have access to such sensitive data have met the employee requirements noted in the following section. The business contact is also responsible for immediately notifying Merchant Services of any employee turnover including the business contact's immediate supervisor.

Off-Boarding Process for Merchant Locations

It is imperative to complete and submit the Off-Boarding a Merchant Employee form if an employee's duties change or is no longer working for the department or University.

The business contact must also complete and submit the Cancellation of Merchant Services form in the event that your department will no longer process payment card transactions. Refer to section Device Protection, Inspection & Disposition for additional requirements.

Employee Requirements

The unit's business contact, technical contact, and merchant employees that will have access to sensitive payment card information and/or will record the merchant deposits in the general ledger must be approved by the Controller's office. The Merchant Employee e-form initiates the on-boarding employee process.

To complete such process, the following requirements must be met:

1. Undergo and clear an Expanded Background Check
2. Complete the PCI Training for Merchants or PCI Training for IT upon hire and annually and pass with a score of at least 80%.
3. Complete the annual Security Awareness training.
4. Complete the Employee Statement of Understanding form.
5. Complete training according to the applicable approved method noted below:
    - Terminal: Once the equipment is received, the training will be conducted over the phone with the respective representative.
    - Internet (E-Commerce): only CyberSource: Online training is available via tutorials, setting-up a test account, and access to supporting documentation. Existing merchants may contact CyberSource customer support at 1-866-5017958.

- Third-party Vendor (POS, E-Commerce, Payment Applications, and Software): Merchant will also be responsible for coordinating training with the vendor and to ensure access is granted on a business need-to-know basis.

6. The assigned journal contacts for each merchant location must register, complete and pass the Merchant Journal Training to be granted journal access in PeopleSoft.

Once an employee has been approved by Merchant Services via the Merchant Employee eform workflow they are considered a Merchant Employee.

Engaging a Third-Party Vendor

Before establishing a relationship with a third party service provider (TPSP) that stores, processes, transmits cardholder data, or could impact the security of the cardholder data environment (CDE), a department must obtain approval from the PCI Compliance Team via the Total Contract Manager (TCM) tool. A vendor must have the ability to demonstrate that they are PCI DSS compliant.

The following TPSP vendor checklist will assist your department in requesting the appropriate documentation from the vendor prior to contract approval/renewal. Any deviation from or omission of the below documentation may be acceptable, but only if it is approved by the PCI Compliance team.

- Attestation of Compliance (AOC)
- Ensure one of the following PCI Language templates are embedded in the contract and/or supplemental documentation as it applies.

Non-Software related Agreements

Compliance with PCIDSS: Vendor will ensure all services are delivered in full compliance with the most recent version of the Payment Card Industry Data Security Standard (PCI-DSS) in effect at the time of service delivery. Vendor will treat all FIU provided infrastructure and resources as public and non-secure, regardless of measures FIU may choose to put in place. Vendor will also maintain all required qualifications and periodically furnish proof of ongoing compliance in the form of an Attestation of Compliance to demonstrate to FIU that Vendor is continuously operating in full compliance with PCI-DSS and is not relying on FIU for any aspect of that compliance. If Vendor loses any required certification or this lapses, Vendor shall immediately notify FIU, and FIU will have an option to terminate this contract for convenience, seeking a refund for any unrendered services.

Software License Addendum

PCI-DSS: as may be applicable, deliver all services in full compliance with the most recent version of the Payment Card Industry Data Security Standard (PCI-DSS) in effect at the time of service delivery. Vendor will treat all FIU provided infrastructure and resources as public and non-secure, regardless of measures FIU may choose to put in place. Vendor will also maintain all required qualifications and periodically furnish proof of ongoing compliance in the form of an Attestation of Compliance to demonstrate to FIU that Vendor is continuously operating in full compliance with PCI-DSS and is not relying on FIU for any aspect of that compliance. If Vendor loses any required certification or the certification lapses, Vendor shall immediately notify FIU, and FIU will have an option to terminate this contract and receive a refund for unrendered services."

Competitive Solicitation- Invitation to Negotiate (ITN) Template Language

PCI DSS. Successful Respondent represents and warrants that for the life of the Contract and/or while Successful Respondent has involvement with FIU customer cardholder data, the software and services used for processing transactions shall be compliant with the most recent version of the Payment Card Industry Security Standards Council (https://www.pcisecuritystandards.org/) in effect at the time of service delivery. Successful Respondent will treat all FIU provided infrastructure and resources as public and non-secure, regardless of measures FIU may choose to put in place. Successful Respondent will also maintain all required qualifications and periodically furnish proof of ongoing compliance in the form of an Attestation of Compliance to demonstrate to FIU that Successful Respondent is continuously operating in full compliance with PCI-DSS and is not relying on FIU for any aspect of that compliance. Successful Respondent shall, upon written request, furnish proof of compliance with PCI DSS within 10 business days of the request. Successful Respondent agrees to provide to FIU a current and complete copy of their Attestation of Compliance (AOC). Further, Successful Respondent agrees to provide to FIU proof of a recent (no more than 3 months old) passing quarterly external vulnerability scan as submitted by an Approved Scanning Vendor (ASV). If Successful Respondent loses any required certification or the certification lapses, Successful Respondent shall immediately notify FIU, and FIU will have an option to terminate this contract and receive a refund for unrendered services. Successful Respondent further agrees to comply with FIU's Payment Card Processing Policy (see FIU Policy 1110.025, as it may be updated).

Processing Best Practices

Card Processing and Collection

- Do not share payment card information via e-mail, voice message, or instant message. If the information is received via an authorization form by mail, telephone or secured fax, the transaction must be processed within one business day from when the user has access to the cardholder information. The cardholder's sensitive information must be cross-cut shredded immediately after processed.
- Never store the 3-digit authorization code (primarily found on the back of the card) after the credit card payment has been processed.
- Truncate the primary account number (PAN) when displayed (only last four digits are the maximum number of digits to be displayed).
- Permit only employees who have a legitimate "need-to-know" access to cardholder information.
- All terminals should auto-batch; however, if not, settle sales at the end of each day to secure next day funding.
- No individual should be processing payments and refunds/voids, refer to the segregation of duties section.
- For card-not present transactions, it is crucial that you require the customer to enter or provide their CVV/CSV code and zip code as this process will provide additional authentication and prevent some fraudulent transactions from occurring.

Segregation of duties

Segregation of duties must be established between payment card processing, the processing of refunds and voids, and reconciliation of revenue.

- Credit card payment processing function must be segregated from processing a credit or refund.
- Credit card payment processing function must be segregated from processing of a void.
- Credit card payment reconciliation function must be segregated from processing payments, voids, credits and refunds.

If the department has insufficient personnel to implement such segregation of duties, then a refund/void must be approved by a supervisor or department head by signing the refund /void receipt attached to the original transaction receipt. The same approval must be documented for the reconciliation function as well.

Data Storage and Destruction

- Storage of cardholder data is NOT permitted.
- Any documents that contain card information must be cross-cut shredded immediately upon processing of payment.
- Redacting payment card data on written documents is acceptable if the card number, expiration date, and security code are cut off the form and immediately cross cut shredded.

Responding to e-mailed cardholder data (CHD)

Any open communication system such as email or chat programs are not considered secure for the transmission of any payment card information. If a client should send their payment information to the department, the following steps should be taken:

1) Click "Reply" on the email.
2) Delete the payment card data from the original portion of the email.
3) In your response, Copy and paste the following:
    a. "Thank you for contacting (*insert department or name)*. We appreciate your business, however as part of our compliance effort with the Payment Card Data Security Standard and our practice to protect all of our customers' Personally Identifiable Information, we cannot process the payment that you have sent through email. We ask that you use one of the following approved methods for making your payment:
        o Online - www.xxxxxxxxxx.edu o
        Mail – mailing address
        o Phone – xxx-xxx-xxxx
        o Fax – xxx-xxx-xxxx
4) Then promptly delete the original email and empty the trash.

Suggestion Verbiage to Add to Form

"For your protection, please do not e-mail this form with your credit card information as the payment will not be processed. Please contact us directly at (phone number) and we will gladly assist you."

Device Inventory and Inspection Logs

A complete inventory of PCI devices and components must be kept current by the Primary Business Contact. Any changes made to the PCI devices inventory will be reflected on your Merchant Device Inventory Sheet and Tampering Checklist immediately and a copy uploaded into

your assigned OneDrive folder monthly. The purpose of the checklist is to assist merchant locations in complying with a requirement of the PCI DSS. This is to be completed on a regular basis by departments that process credit card payments via a terminal and/or similar point of sale device. The device(s) must be inspected and logged prior to processing your first card transaction for the day.

The PCI Compliance team recommends you incorporate this process in your opening procedures to ensure the front-line staff are completing the log. Inspection of the device is not required if the device is not in use. Please upload the document to your assigned merchant OneDrive folder at the beginning of the month for the previous month's logging history.

Device Protection, Inspection, and Disposition

Report suspicious behavior, indications of device tampering, or device replacement immediately by contacting the PCI Compliance team via email at pcicompliance@fiu.edu.

Protection

- The risk of tampering, replacement or theft of point-of-sale terminals grows when these devices are left unattended.
- Keep the terminal(s) out of customers and unauthorized personnel's reach.
- Only allow terminal repairs from authorized personnel and only if you are previously notified by Merchant Services.
- Install terminal updates as instructed.
- Do not move terminal from the VLAN (private secure FIU network).
- Maintain an internal Merchant Location Visitor log which must be uploaded along with the other documents on a monthly basis, if applicable.

Inspection

- Regularly check your terminal to verify that it has not been tampered with and incorporate into your opening day procedures.
- If your device has a method of displaying the serial number for the device, check that the serial # on the back of device matches the serial number you have in your internal list.
- Inspect the device for any additions you may not recognize such as small skimming devices or key loggers that could be attached to the device.
- Inspect the wires and connections to the terminal for anything unfamiliar.
- Check for any unfamiliar devices around the work area. Smartphones should not be utilized near any credit card device to prevent potential capturing of credit card data.
- Inspect the surrounding area for the terminal, looking for possible cameras that may have been added (these can often be very small and easy to hide).
- Log the information into the Merchant Device Inventory and Tampering Checklist and upload document into your assigned OneDrive folder.

Disposition

- It is mandatory to return obsolete terminals to the Office of the Controller in order to clear the memory and securely dispose of the device. Contact Merchant Services to complete this task.

Incident Response Plan

Follow the process below in the event of a credit card security breach or incident:

- Notify your supervisor and the PCI Compliance Team via email at pcicompliance@fiu.edu immediately.

Recording of Merchant Activity

Deposits

Merchant Services implemented an interactive training to assist journal contacts in creating entries related to payment (debit and credit) card activity in PeopleSoft Financials. The training provides resources that will further facilitate the recording process. The training can be accessed by enrolling in the Merchant Journal Training under the Office of the Controller.

Refunds

Establish a refund policy that will limit acceptance of returned merchandise and canceled services, or that your location will allow refund adjustments contingent on certain requirements.

In a retail business, it's a good idea to noticeably display your return and exchange policies in the store, and it is also a requirement to print them on sales receipts. Some card issuers do not require you to refund a transaction if your policies are clearly made known and posted as either of the following:

- No Refund
- Exchange Only
- In-store credit only, if applicable

Whichever policy you select must appear in letters approximately ¼ inch high and in close proximity to the space provided for the Cardholders signature and the transaction must be signed by the Cardholder.

For online locations, you must have your refund policy available on your website through a clearly visible link on your homepage. Customers should be able to click on an "Accept or I agree" button to acknowledge they have read and understand the refund policy.

In addition, refunds must be issued using the same mode of processing that was used for the original transaction and to the same payment card number. If the cardholder can provide documentation that the original payment card account number has been closed, the department may issue a refund to another payment card assigned to the cardholder. The refund amount cannot exceed the original transaction amount.

Chargebacks

A chargeback is a processed credit card transaction that is reversed (charged back) to a merchant because the customer or customer's bank finds something wrong with the transaction. There are several reasons a transaction can be reversed:

- Authorization error: A transaction was allowed even though the authorization was declined.

- Processing error: Incorrect calculation on the sales draft, invalid account number, or expired card.
- Customer disputes: The customer denies taking part in the transaction, claims purchased merchandise or services were never received and an attempt was already made to resolve the dispute, mail order merchandise was defective, or a promised credit was never processed.

Chargeback issued by American Express

Merchant Services will notify you via e-mail of your recent chargeback/dispute if issued by American Express. However, it is the responsibility of the department to contact AMEX to dispute their claim. It is imperative that your department maintains accurate record keeping and files documentation accordingly.

Chargeback issued by Bank of America Merchant Services (BAMS)

Bank of America Merchant Services has an online portal called Business Track that provides merchants with a quicker route to respond to chargebacks. The supporting documentation to dispute a chargeback is submitted electronically in the portal. Below is the information needed to self-enroll into BAMS Business Track.

- Click on the hyperlink: https://www.businesstrack.com
- Click on "Create an Account"
- Click on "Sign up with your Merchant Account

Then, you will be required to input the following information to create an account:

- Merchant #: (12 digits)- "Enter your MID" (If you have more than one MID, enroll for each separate one)
- Business Checking Account #:
- Tax ID: 650177616

Each merchant location should have a dedicated staff member responsible for handling chargebacks.

Record Retention

All merchant locations are required to adhere to the State of Florida's general records schedule GS1-SL. The item numbers below can be located within the GS1-SL schedule:

- Signature Authorization Records (Item #300): This record series consists of forms authorizing individuals to sign purchase orders, credit cards/receipts, or paychecks, to accept packages requiring a signature, or to sign off on other types of agency business. **RETENTION: 1 fiscal year after obsolete or superseded**
- Receipt/Revenue Records: Detail (Item #365): This series consists of records documenting specific receipts/revenues collected by an agency through cash, checks, electronic transfers, credit and debit cards, or other methods. The series may include, but is not limited to, records such as cash collection records and reports, cash receipts books, cash register tapes, deposit transfer slips, EFT notices, credit and debit records receipt

ledgers, receipt journal transactions and vouchers, refund records, bad check records, and other accounts receivable and related documentation. Retention is based on Section 95.11(2), Florida Statutes, and Statute of Limitations on contracts, obligations, or liabilities.
RETENTION: 5 fiscal years

- Payment Card Sensitive Authentication Data (Item #395): This record series consists of elements of a customer's payment card data that are used to authenticate a financial transaction using that payment card (e.g. credit card, debit card). Sensitive authentication data includes those elements defined as such by the Payment Card Industry Security Standards Council in their Data Security Standard. Requirements and Security Assessment Procedures (Version 1.2, October 2008 or subsequent edition) and includes full magnetic stripe data (also known as full track, track, track 1, track 2, magnetic-stripe data); three-digit or four digit card verification code or value; and personal identification number (PIN) or encrypted PIN block.
  RETENTION: Destroy immediately upon completion of the transaction.

Roles and Responsibilities

Below are all the departments involved in this effort to achieve and maintain PCI compliance.

Office of the Controller – responsibilities include:

- Assist merchants with assessing their business process for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto.
- Verifying those merchants comply with this policy, PCI DSS, and University policies defined in "Related Information" regarding business process for payment card processing.
- Overseeing the policies and procedures on payment card processing including issuance of merchant number and revocation of merchant number if merchant fails to comply with this procedure.
- Review and approve third party vendor contracts that are related to the University handling cardholder data and/or when FIU acts as a service provider.

Division of Human Resources – responsibilities include:

- Conduct appropriate level of background checks for employees who will have access to, or otherwise handle, cardholder information upon the department's request consistent with applicable laws and University policies.

Division of Information Technology – responsibilities include:

- Assist merchants with assessing information technology assets for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto.
- Verifying those merchants comply with this procedure, PCI DSS, and University policies defined in "Related Information" regarding information technology assets for payment card processing.
- Operations and maintenance of the FIU data networks and the establishment of information technology security policies and standards.
- Perform internal vulnerability scans, if applicable.
- Review vendor contracts which deal with credit card data and PCI.
- Assist with the selection of validated P2PE devices.
- Provide security awareness training reports.

- Overseeing the conduct of internal and external cardholder data environment controls at the appropriate intervals.
- Work with QSA and Controllers Office to review SAQs for attestation of PCI compliance.

Office of the General Counsel (OGC) – responsibilities include:

- Review merchant related contracts that apply based on dollar thresholds
- Review e-commerce refund and privacy policies.

All University Departments (PCI Compliance obligations)

This applies to any department that engages with a Third Party vendor or Tenant that is the merchant of record (MOR) - responsibilities include:

- Ensure that vendors that are connected to the FIU network are PCI DSS compliant.
- Oversight of new and existing vendors/tenants that process payment cards.
- Engage the PCI Compliance Team for review and approval of new or existing vendor contracts from a PCI DSS compliance perspective.
- Annually obtain the Attestation of Compliance (AOC) from third-party vendors and communicate information to the PCI Compliance Team.

Merchants (University Department) – responsibilities include:

- Analyzing your business process and technical components for improvements.
- Timely remediation of vulnerabilities.
- Compliance reporting of annual forms, questionnaires, on-site reviews, third-party vendor verification, on-boarding employee verification, timely removal of any employee access, etc.
- Notify the PCI Compliance Team immediately in the event of any suspected payment card processing security breach, including those of any vendor or tenant.
- Users processing credit cards and users with access to cardholder data are required to complete the IT Security Awareness training and the PCI training annually.
- Comply with the payment card processing policy and PCI DSS.

Internal & External Merchant Location Reviews

Annual Review

- Annual training is required to retain job duties involved with handling credit/debit card payments for active merchant employees.
- The completion of the self-assessment questionnaire (SAQ).
- Ensure any third-party vendors have furnished validation documentation such as an AOC.
- Review current departmental procedures to ensure your merchant process has not changed.

Quarterly Review

- Internal and external vulnerability scans, if applicable.

Periodic Review

- The Office of the Controller reserves the right to conduct announced and unannounced periodic field reviews of any merchant location.

On-going Review

- Maintain an internal list of merchant employees (Listing of all staff involved with accepting or handling payment cards).
- Maintain Inspection Logs of all Payment Card Processing Equipment.
- Maintain Inventory of all devices used for inputting cardholder data.

Merchant Location Consequences of Non-Compliance

All alleged violations will be thoroughly reviewed by Merchant Services and/or the PCI Compliance team. Additional information will be requested from the Merchant Location's (department) Primary Contact prior to enforcing the following consequences of non-compliance. Failure to comply with the requirements noted in the Payment Card Processing policy or the Merchant Services PCI DSS Compliance Manual may result in the following violations:

Initial Violation Notification (Issue Identified)

An email notification detailing the issue(s) will be sent to the Merchant Location's Primary Contact and/or the Primary Journal Contact and/or the Merchant Employee, and may also include the back-up journal contact, Supervisor (if different), as deemed appropriate. The employee will be required to make adjustments to become compliant.

Examples include:

1. The Journal Contact did not record the appropriate journal(s) in a timely manner (i.e. within 2 business days of the sale).
2. Primary Contact failed to submit the required documentation (i.e. monthly merchant inventory and device tampering checklist log).
3. Employee identified as having access to cardholder data prior to becoming approved.
4. Employee failed to complete their annual PCI Training within the allowed timeframe.

Second Violation Notification (Failure to Correct Issue within Allowed Timeframe)

An email notification detailing the issue(s) will be sent to the Merchant Location's Primary Contact and/or the Primary Journal Contact and/or Merchant Employee, and will also include the back-up journal contact, Supervisor (if different) and/or the Dean/Department Head, and the PCI Compliance Team, as deemed appropriate. The employee will be required to make adjustments and potentially complete training to become compliant.

Examples include:

1. The primary and/or back-up journal contact did not record and/or revise the corresponding journal(s) within the deadline provided (i.e. prior to the deadline provided by the Merchant Services team).
2. Primary Contact failed to submit the required documentation within the deadline provided (i.e. monthly merchant inventory and device tampering checklist log).
3. Employee failed to complete their annual PCI Training within the new deadline provided.

Third Violation Notification (Failure to Correct Issue and Last Reminder)

An email notification detailing the outstanding violation(s) will be sent to the Merchant Location's Primary Contact and/or the journal contact(s) and/or the Merchant Employee, Supervisor (if different), and the Dean/Department Head, and the PCI Compliance Team, as deemed appropriate. The employee will be required to re-take certain trainings depending on the reason for the violation.

Examples include:

1. Journal Contact's Peoplesoft access to create/edit credit card journals will be revoked until the requirement of completing and passing the Online Merchant Journal Training is fulfilled.
2. Primary Contact failed to submit the required documentation and a hard deadline is given to the merchant notifying the team that their merchant account will be disabled if non-compliant.
3. Employee failed to complete their annual PCI Training within the extended deadline provided.

Fourth Violation Notification

A final email notification will be sent to the Merchant Location's Primary Contact and/or the journal contact(s) and/or the Merchant Employee, Supervisor (if different), and the PCI Compliance Team, as deemed appropriate. Actions taken for failure to comply will be dependent upon the nature of the violation and up to the final discretion of the University Controller.

However, when the violation is due to failure to complete the annual PCI Training, the non-compliance issue will be escalated to Human Resources to determine appropriate discipline.

The PCI Compliance Team reserves the authority to make changes or modify the above procedures. Based on the severity of the infraction, your merchant account may be disabled and/or your access may be revoked regardless of the number of violations on file.

Contact Information

	Contact Number	Email Address
FIU PCI Compliance Team		pcicompliance@fiu.edu
FIU Merchant Services	305-348-3888	merchant@fiu.edu
FIU Information Security Office	305-348-1366	security@fiu.edu
AMEX Customer Support	1-866-220-4272	
Bluefin Payment Solutions Customer Support	1-800-675-6573	service@bluefin.com
CyberSource Customer Support	1-866-501-7958	
BAMS Customer Support	1-800-430-7161	
Clientline Customer Support	1-800-285-3978	Reporting tool demo

Related Links

- 1110.025 Payment Card Processing: https://policies.fiu.edu/policy/728
- 1930.020b IT Security Procedure: Sharing Access To IT Resources: https://policies.fiu.edu/policy/559
- Visa's Global Registry of Service Providers http://www.visa.com/splisting/
- PCI Council's Website: https://www.pcisecuritystandards.org/document_library?category=saqs
- Merchant Services Website: https://controller.fiu.edu/departments/accounting-reporting/merchant-services/

Glossary of PCI DSS Definitions and Related Terms

Acquirer – Also referred to as "acquiring bank" or "acquiring financial institution". Entity that initiates and maintains relationships with merchants for acceptance of payment cards.

Approved Scanning Vendor (ASV) – Company approved by the PCI Security Standards Council to conduct scanning services to identify common weaknesses in system configuration.

Business Need-to-Know - When an employee's access rights are granted to only the least amount of data and privileges needed to perform a job.

Cardholder Data – At a minimum, cardholder data contains the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, service code, and/or other sensitive authentication data.

Cardholder Data Environment (CDE) – Area of computer system network that processes cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

Data Breach – A data breach is an incident in which sensitive data may have potentially been viewed, stolen, or used by an unauthorized party.

FIU Network – The FIU Network is a high-performance series of interconnections which connects the FIU community, providing access to departmental computing resources, FIU system resources, as well as Internet connectivity. The network enables any person and/or device with network connectivity access to any FIU service both on-and off-campus. The network is designed to be highly reliable and operational 24 hours a day, 365 days a year.

Malware – Malicious software designed to infiltrate a computer system with the intent of stealing data, or damaging applications or the operating system. Such software typically enters a network during many business approved activities such as via email or browsing websites.

Merchant – A University department approved to accept payment cards at a given location as payment for goods and/or services or receipt of donations.

Merchant ID Number (MID) – A unique number that identifies the University department approved to accept payment cards.

Payment Card Application – Any hardware, software, or combination of hardware and software that aid in the processing,
transmitting or storing of cardholder data as part of authorization or settlement. Examples include: point of sale (POS) devices, ecommerce shopping carts, web-based payment applications and third party (vendor) provided systems.

Payment Card Industry Data Security Standard (PCI DSS) – PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC)- The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI DSS may be accessed at: https://www.pcisecuritystandards.org/.

Self-Assessment Questionnaire (SAQ) –A validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple versions of the PCI DSS SAQ to meet various payment card processing scenarios. Each unique version of the PCI DSS SAQ includes a Self-Assessment Questionnaire and Attestation of Compliance, which must be completed annually by the merchant and/or service provider as appropriate. The FIU PCI Compliance Team will assist you in the selection and completion of the SAQ for your merchant location.

Payment Card Processing – The processing, transmitting and/or storing of cardholder data, i.e. acceptance of credit or debit cards.

Primary Account Number (PAN) – Unique number for credit and debit cards that identifies the cardholder account.

Qualified Security Assessor (QSA) – A company approved by the PCI Security Standards Council to validate an entity's adherence to PCI DSS requirements.

Service Provider – A business entity that provides various services to merchants. Typically, these entities store, process, or transmit card data on behalf of another entity (such as a merchant) OR are managed service providers that provide managed firewalls, intrusion detection, hosting, and other IT-related services.

Vulnerability Scan – A software tool that detects and classifies potential weak points (vulnerabilities) on a computer network.