PCI @ GVSU

PCI Training for GVSU Employees

This training will help explain the requirements for PCI compliance for Grand Valley State University in order to accept credit cards.

Next →

What is PCI?

PCI stands for Payment Card Industry and refers to PCI DSS (Payment Card Industry Data Security Standard), a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

- Consists of 12 requirements, including protecting cardholder data, access control, and logging.
- GVSU must submit yearly evaluations, via a Self-Assessment Questionnaire (SAQ) to verify our compliance with PCI DSS.
- Compliance with PCI DSS helps prevent data breaches and protects both customers and businesses from fraud.
- Each department accepting credit cards is considered a merchant in PCI terms.

← Previous | Next →

GVSU PCI Environment

Information on specific elements of GVSU's PCI environment are found below, please click the title to expand.

Why We Must Follow PCI Requirements

Failure to follow PCI requirements can have serious financial and reputational consequences. Organizations that do not properly protect credit card data can become a source of stolen credit card information, placing customers at risk of fraud and identity theft.

If a breach occurs, the University may be held financially responsible for resulting losses. This can include paying regulatory fines, covering fraud-related losses, and absorbing the costs of credit card replacement for affected individuals. Adhering to PCI standards helps protect our customers, reduce institutional risk, and ensure continued trust in University systems.

PCI Compliance Officer and Committee

The responsibility for maintaining PCI compliance at Grand Valley State University resides with the PCI Compliance Officer and the PCI Committee. Together, they oversee University-wide compliance efforts and ensure that credit card processing aligns with PCI DSS requirements.

The PCI Compliance Officer is:

- Luke DeMott

The PCI Committee includes:

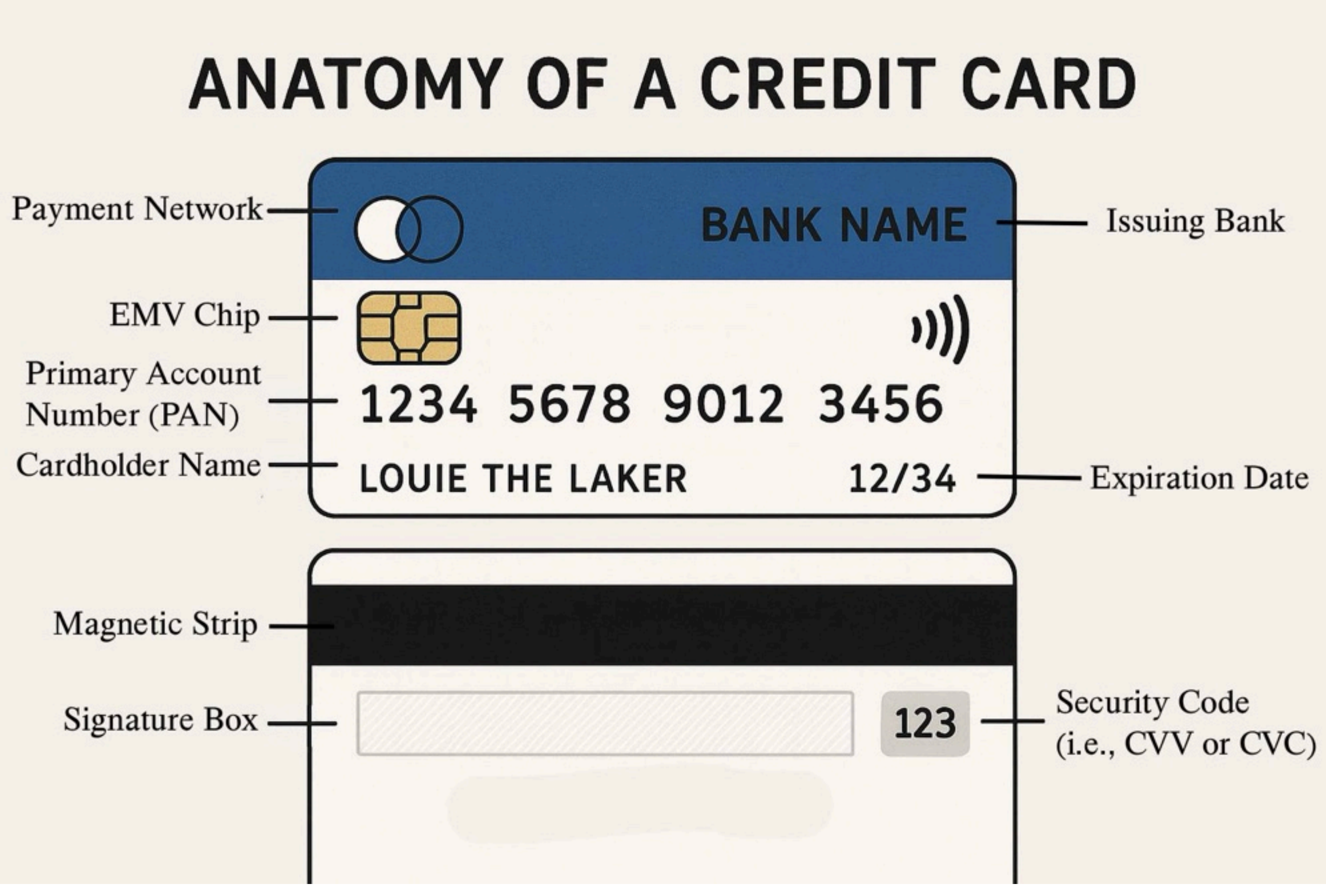
- Luke DeMott
- Chad Reynolds
- David Van Sweden
- Brad Vedders
- Greg Vedders

The PCI Committee is responsible for reviewing and approving software and vendor requests related to credit card processing. Each year, the PCI Committee completes and submits the required Self-Assessment Questionnaires (SAQs) on behalf of all GVSU merchants. These submissions are informed by feedback gathered through

> the annual PCI survey, along with additional evaluation data collected throughout the year. This centralized process ensures consistency, accuracy, and compliance across all University departments that accept or process payment cards.
>
> PCI responsibilities and guidelines are available at: https://gvsu.edu/pci

← Previous | Next →

Credit Card 101



All credit cards contain the same essential information, though the placement of these elements may differ depending on the issuing bank and card design. The key components include:

- Issuing Bank – The financial institution that provides the card and manages the account.

- Payment Network – The brand that processes the transaction (e.g., Visa, Mastercard, Discover, American Express).
- Primary Account Number (PAN) – The 15–16 digit number that identifies the cardholder's account.
- Cardholder Name – The authorized user's name as it appears on the account.
- Expiration Date – The month and year the card is valid through.
- EMV Chip – A secure, embedded microchip used for encrypted transactions.
- Magnetic Stripe – Contains encoded account data for swiping at compatible terminals.
- Signature Box – A space for the cardholder's signature, used for verification.
- Security Code (CVV or CVC) – A three- or four-digit code used as an added authentication factor for card-not-present transactions.

← Previous | Next →

Types of Transactions

Credit card transactions can occur in several different ways, depending on how the customer and merchant interact. Face-to-face, or "card-present," transactions happen when the customer is physically present and hands their card to the merchant or taps/inserts it at a terminal. These are generally considered the most secure because the card and cardholder can be verified in person.

In contrast, Mail Order or Telephone Order (MOTO) transactions occur when the customer is not physically present. The merchant manually types or "hand-keys" the card number into their system based on information provided over the phone or through mailed forms. Because the card isn't present, these transactions carry higher fraud risk and typically require additional verification steps.

Finally, e-commerce transactions take place online when a customer enters their own payment information into a website or app. The merchant never handles the card directly; instead, the customer submits details through a secure checkout process. These are also considered "card-not-present" transactions and rely on digital security tools—like encryption, address verification, and CVV checks—to reduce fraud.

← Previous | Next →

What Are Our Responsibilities?

As part of Grand Valley State University's commitment to protecting payment card information, every individual involved in processing, handling, or supporting cardholder data plays an essential role in maintaining PCI-DSS compliance. These responsibilities are not optional—they are required safeguards that ensure we uphold the security, trust, and integrity of the University's payment operations.

This section outlines the expectations for all personnel who interact with the PCI environment. By understanding and following these responsibilities, we help prevent unauthorized access, reduce institutional risk, and ensure that GVSU meets all regulatory and audit requirements.

- Never store physical credit card information or retain full credit card data in any form
- Each user is responsible for understanding how PCI requirements apply to their specific role. Users should work with their supervisor to determine and confirm their responsibilities related to credit card handling and PCI compliance.
- Ensure all credit card processing websites use HTTPS in the browser address bar.
- Maintain internal policies and procedures to protect cardholder data see https://gvsu.edu/pci for more information.
- Ensure newly onboarded personnel are informed of PCI requirements and complete required training.
- Any credit card number, whether written or electronic, that is temporarily stored must be secured immediately and either kept in a locked cabinet with restricted access or permanently deleted or destroyed as soon as it is no longer needed, using PCI-compliant secure deletion methods for electronic data or a PCI-compliant shredder for physical media.
- Use a different password than your regular GVSU account.
- Complete a daily visual inspection log of PCI-related equipment on each workday when the credit card reader is used to process credit card transactions to check for signs of tampering, skimmers, or other suspicious activity. Additional information on what to look for is available at https://www.gvsu.edu/cms4/asset/9539BEE0-AB4D-AD66-BE5FF618A6CA0752/terminalinspectionguide.pdf.
- Report suspected or confirmed security incidents to security@gvsu.edu.
- Submit change requests via the form available at https://www.gvsu.edu/pci
- IT staff must update the PCI Change Log anytime the PCI environment is modified.

In-scope systems include any systems, applications, or devices that store, process, or transmit credit card data, as well as any systems that are connected to or can impact the security of those systems. These assets are subject to PCI DSS requirements and must follow all applicable security controls and monitoring standards.

← Previous | Next →

Reporting a PCI Security Issue

When a potential credit card data incident is suspected, it is critical to act quickly to limit exposure, preserve evidence, and ensure proper notification and reporting.

Identify and Contain the Incident

The first priority is to identify the incident and prevent further damage. This includes recognizing any unusual or unauthorized activity involving cardholder data and taking immediate steps to preserve evidence. Systems involved in the incident should not be powered off or altered; leave affected computers on and avoid deleting or modifying any data.

To contain the breach, affected systems should be isolated as soon as possible. For example, disconnect the Ethernet cable from the network jack or otherwise remove network access to prevent additional data exposure.

Notify Key Internal Stakeholders

Once the incident is identified and contained, appropriate University contacts must be notified immediately.

- Alert the organization’s PCI Compliance Officer, Luke DeMott, or the designated security team
- Email **security@gvsu.edu** or contact any PCI Committee member directly
- The PCI Committee will engage IT or cybersecurity professionals to assess the scope of the incident

- The PCI Committee will notify external entities as required

Comply with Legal and PCI DSS Reporting Requirements

The University must meet all legal and regulatory obligations following a credit card data incident.

- The PCI Committee will report the incident to law enforcement or regulatory authorities, as required PCI-specific reporting requirements will be followed, including:
    - Notifying the acquiring bank or payment processor
    - Submitting an Incident Response Report to appropriate PCI DSS stakeholders

Communicate with Affected Parties

If necessary, affected customers or stakeholders will be notified in a timely and transparent manner. Communications should include information about the nature of the incident, steps being taken to address it, and recommended actions such as monitoring accounts or updating passwords.

Review and Improve the Incident Response Process

After the incident has been resolved, a post-incident review will be conducted to evaluate the effectiveness of the response. The PCI DSS Incident Response Plan will be updated as needed to address any gaps, strengthen controls, and improve future response efforts.

← Previous | Next →

Prohibited Practices

To protect cardholder data and ensure GVSU remains fully compliant with PCI-DSS requirements, certain actions are strictly prohibited. These practices create significant security risks, expose the University to potential data breaches, and may result in loss of payment card processing privileges. All staff who handle, process, or support credit card transactions must understand and avoid the activities listed below.

Credit Card Handling

- Storing CVV/CVC codes, pin numbers, track data or card numbers (either electronically or on paper).
- Never take a picture of a credit card.
- Sending credit card information via mobile or end-user messaging technologies (email, fax, text).
- Repeating a credit card number to a customer over the phone. Always ask them to repeat if needed.
- Entering credit card information into a GVSU website on behalf of a customer.

Physical Mail

- Requesting credit card information to be sent to a non-PCI specific GVSU postal address.
- Sending credit card information via intercampus mail.

Hardware

- Using a non-PCI or Point to Point Encrypted (P2PE) compatible device for entering credit card information.
- Using non-approved third-party service providers to process credit card transactions.

- Use of Square Payments or other swipe devices or applications without prior approval is not permitted.
- Using non-designated PCI compliant shredding devices or services.

← Previous | Next →

New Software and Systems

Any new contract or business relationship that involves the acceptance, processing, or handling of credit card payments must undergo a formal review process before it can be finalized. These arrangements are required to be reviewed by Information Technology (IT) and Business & Finance, and must receive approval from the PCI Committee prior to signing any contract.

To support this process, onboarding procedures for new PCI vendors are available on the University's PCI website (https://gvsu.edu/pci). Departments should work closely with Chad Reynolds and David Van Sweden throughout the review to ensure the vendor meets all PCI compliance requirements and aligns with University security standards.

← Previous | Next →

Accepted Processing Procedures

GVSU offers several options for accepting credit cards. The options outlined below represent common credit card processing scenarios used across the University and are intended to help departments identify an approach that aligns with their operational needs while maintaining compliance with PCI requirements.

GVSU Ecommerce

For campus units that need to accept credit card payments, several secure options are available depending on the volume and nature of the transactions. Departments that regularly process payments through their websites should use approved secure websites, managed in partnership with University Marketing. CMS site owners can integrate payments by using the e-commerce form element within Form Builder. For assistance with these online tools, Josh Isaak in University Marketing (ext. 8605) serves as the primary contact.

Third Party Service Providers

Please contact Chad Reynolds in the Accounting Business Office (ext. 9484) to discuss available and approved third-party service provider (TPSP) options for credit card processing. A TPSP is a vendor that securely handles credit card transactions on behalf of the University, which can reduce risk, limit exposure to sensitive cardholder data, and simplify PCI compliance requirements.

Physical Device

Units that need a physical point-of-sale device may use an approved secure terminal, available in both wired and cellular models. These devices meet University and PCI security requirements. To purchase a terminal or determine the best model for your needs, contact Chad Reynolds in the Accounting Business Office (ext. 9484).

Loaner Terminal(s)

For day-of-event registrations, departments may request the use of a loaner terminal to process credit card transactions on site. These terminals must be reserved in advance, with requests submitted to the Bank Desk at least three days before the event.

Loaner terminal request forms and additional details are available on the University's PCI website (https://gvsu.edu/pci).

Low Volume

For low-volume or call-in payments, departments may choose to route customers directly to designated offices that can process credit card transactions on their behalf. For gift-related payments, calls can be transferred to Gift Processing/Development at ext. 6086, along with the appropriate Worktags. For all other non-tuition payments, calls may be transferred to the Business and Finance office at ext. 2233.

Mail

If payments arrive through U.S. Mail, the University maintains a dedicated PO Box to support secure handling. Departments may temporarily write down credit card information for processing, but this information must be destroyed immediately afterward using a PCI-compliant shredding method. Only cross-cut or diamond-cut shredders that meet PCI security standards—or an approved shredding service—may be used to ensure sensitive information is properly disposed of.

NOTE: GVSU does not allow the storage of full credit card numbers. Only the last four digits may be retained, as permitted by PCI regulations.

← Previous | Next →

PCI Fees

At Grand Valley State University, departments are not permitted to directly pass credit card processing fees to customers who choose to pay by credit card. This means no separate surcharge or line-item fee may be added specifically for credit card payments.

However, departments may set their overall rates with the understanding that credit card processing fees typically range from 2–3%. When establishing pricing, departments should account for these costs across all forms of payment, rather than applying a fee only to credit card transactions.

This approach ensures compliance with University policy and maintains consistent, transparent pricing for customers.

← Previous | Next →

PCI Review

Complete the questions below to check your understanding and reinforce key concepts.

Which of the following is a reason not to comply with PCI DSS rules?

○ Adhere to industry standards

○ Ensure Grand Valley State University is secured against financial penalties

○ We are not handling credit card information

○ Ensure customer data is handled securely

Which type of data is protected under PCI DSS?

○ Student ID numbers

○ Social Security numbers

○ Credit and debit cardholder data

○ Email addresses

If you have a credit card reader you do not need to check for tampering every business day.

○ True ○ False

Which of the following is considered cardholder data?

○ Cardholder name

○ Primary Account Number (PAN)

○ Expiration date

○ All of the above

Who must comply with PCI DSS requirements?

○ Only banks

○ Only online retailers

○ Any organization that processes, stores, or transmits cardholder data

○ Only large corporations

Score.

Check

The score can't be saved because this page is not part of a SCORM package.

← Previous | Next →

Thank You!

Thank you for taking the time to complete the PCI training and for your continued commitment to protecting sensitive payment card information. We know that these requirements add steps to your daily work, and we truly appreciate your attention to detail and willingness to follow established procedures. Your efforts play an important role in reducing risk, preventing fraud, and maintaining PCI compliance across the University. By staying aware, asking questions when something seems unclear, and consistently applying what you've learned, you help keep GVSU's payment systems secure and protect the trust placed in us by our students, staff, and community.

Thank You,

The PCI Committee

← Previous