PayPal

Sikich

How PayPal can help colleges and universities reduce PCI DSS compliance scope.

Prepared by PayPal and Sikich LLP.

Reduce time and resources needed for PCI DSS compliance.

Campus merchants want to offer multiple payment options to their students, parents, and partners, but complex payment infrastructures can increase security and compliance oversight. This paper explains how PayPal can help higher education institutions limit their responsibilities in order to comply with Payment Card Industry Data Security Standard (PCI DSS) regulations – which can help their IT and finance departments save time and money.

Complex payment infrastructures require more oversight.

Higher education institutions are faced with many challenges when setting up the payment infrastructure for campus merchants such as bursar's offices and bookstores. They must choose systems that can serve a variety of business types, and allow customers to pay with many payment options. In addition, treasury and finance organizations must be able to manage payment systems centrally, while allowing campus business units to operate and customize the payment systems to meet their unique needs.

One of the biggest challenges is maintaining payment security. College and university computer networks continue to be targets for data breaches. Of the top 5 industries suffering data breaches in 2015, education was ranked third, according to Symantec's 2015 Internet Security Threat Report.[1]

Campus IT organizations must protect payment data and personal information, while allowing campus staff to access networks for research and collaboration purposes – and ultimately to enable organizations on campus to be able to receive payments and donations as needed. With growing security threats and greater demand for payment choices, colleges and universities have to devote more resources to network security and payment systems management – and, at the same time, maintain PCI DSS compliance.

PayPal allows your institution to offer payment choices that fit campus business needs, while also helping to limit PCI DSS compliance scope.

The challenges of PCI DSS compliance.

PCI DSS is a comprehensive standard for payment data security with more than 300 requirements and sub-requirements. These requirements include security controls, policies, and procedures that must be in place in the higher education institution's payment card environment in order to achieve compliance.

1 "Putting 2015's Higher Education Cyberattacks into Perspective," *EdTech* magazine, September 23, 2015: http://www.edtechmagazine.com/higher/article/2015/09/putting-2015-s-higher-education-cyberattacks-perspective.

Achieving and maintaining PCI DSS compliance requires a significant commitment of IT resources. PCI DSS best practices recommend that information security and compliance procedures are incorporated into daily activities:

> "To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy."[2]

In addition to achieving and maintaining PCI DSS compliance, institutions must report annually on their compliance activities. Due to the level of merchant credit card activity on campuses, most colleges and universities are eligible to report PCI DSS compliance to their acquirer via a Self-Assessment Questionnaire (SAQ).[3]

The type of SAQ an organization must prepare depends on its payment acceptance method. Each SAQ question relates to a specific PCI DSS requirement. Annual reporting and attestation must cover all of the payment activity on campus that is considered in scope for PCI DSS compliance. Institutions should ask their acquirer about the PCI DSS validation requirements that are appropriate for the payment processing environment.

Properly scoping the payment card environment is critical for effective compliance:

> "The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data."[4]

The cost of achieving and maintaining PCI DSS compliance is related directly to the scope of an institution's CDE. Reducing the scope of the CDE not only reduces the risk of a data breach, but it can also reduce the staff resources and equipment costs necessary for maintaining PCI DSS compliance.

With PayPal, you can set up a hierarchical account structure that provides centralized oversight and a holistic view of payment activity across campus.

Third-party service providers and scope reduction.

As higher education institutions rely more heavily on online and credit card payments, they're working with third-party service providers (TPSPs) to outsource payment solutions and related responsibilities. The services provided by TPSPs range from

2,4 *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2*, Payment Card Industry Security Standards Council, April 2016: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf.

3 "Understanding the SAQs for PCI DSS version 3," PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf.

hosting a secure web page for payment acceptance to offering a fully hosted ecommerce environment. When using the services of a TPSP, institutions should perform due diligence, according to the PCI Security Standards Council:

> "Each organization should develop its own policies and procedures, as well as its own criteria for pre-selecting and managing potential TPSPs during the vetting process. All efforts should be placed on exerting the appropriate amount of due diligence and performing a risk assessment of pre-selected TPSPs."[5]

Using a TPSP may reduce compliance responsibilities in some areas of network and system administration. However, the institution must still have processes in place to manage PCI DSS requirements and annual compliance reporting.

Easier payment processing with PayPal's solutions for higher education.

PayPal is a PCI DSS-validated TPSP that works with institutions to facilitate payment processing on campus, which can help you reduce your compliance validation requirements and better manage ongoing PCI DSS compliance efforts.[6]

PayPal's account management capabilities empower higher education institutions to oversee payment activity and user access at a centralized level, while providing account management functions (such as user privileges) for individual departments. Centralized oversight can help you manage campus merchant activity and maintain PCI DSS compliance.

PayPal's payment solutions allow your institution to offer payment choices that fit campus business needs, while also helping to limit PCI DSS compliance scope.

CENTRALIZED OVERSIGHT.

To manage revenue for several departmental businesses and activities, higher education institutions often have to maintain accounting structures comprised of multiple individual merchant IDs. This decentralized accounting structure creates challenges in administrative reconciliation, treasury management, and compliance efforts. In addition, there are significant ongoing costs associated with maintaining multiple merchant IDs.

With PayPal, you can set up account structures that correspond to departmental hierarchies, general ledger account structures, or custom hierarchical relationships.

5 *Payment Card Industry Security Standards Council – Information Supplement: Third-Party Assurance*, PCI Security Standards Council, March 2016, p. 5: https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf?agreement=true&time=1471303830531.

6 PayPal is fully PCI certified as a Level 1 Service Provider. The certification can be validated on Visa's website on the service provider list by entering PayPal in the search field: http://www.visa.com/splisting/searchGrsp.do.

With PayPal's account management tools, your college or university can set up a hierarchical account structure that provides centralized oversight and a holistic view of payment activity across campus. You can then address the challenges of managing merchant activities across many campus departments. These challenges may involve the following activities:

- Diverse patterns of payment activity related to academic calendars.
- Dormant departmental merchant accounts related to intermittent payment activity for infrequent conferences and events.
- Access privileges for "handed down" or forgotten merchant user accounts that result from staffing changes.
- Merchant ID accounts that are unrecognized at the central administrative level, and therefore are overlooked when updating security features and assessing PCI DSS compliance scope.

Decentralized accounting structures introduce financial, security, and compliance risks. PayPal's administrative account management tools can help your school develop hierarchical user account structures to monitor payments and centrally manage security and compliance.

ADMINISTRATIVE TOOLS FOR SECURITY AND COMPLIANCE MANAGEMENT.

PayPal's administrative tools enable your university's financial representatives to configure PayPal accounts securely, and limit or extend permissions as needed. You can also set up departmental user accounts with administrative access to support user management within a department.

With the appropriate privileges, departmental account administrators can establish controls required for PCI DSS compliance. Here are some examples:

- Implement identification and authentication practices that require the use of unique user IDs, control the addition and deletion of user privileges, and revoke user access upon termination (PCI DSS requirement 8.1).
- Configure user accounts with security keys so you can use multifactor authentication for user access (PCI DSS requirement 8.3).
- Control user privileges that limit access based on a business "need to know" (PCI DSS requirement 7.1).
- Enforce separation of duties between development and production environments for website activation and authorization (PCI DSS requirement 6.4).

HIERARCHICAL ACCOUNT MANAGEMENT.

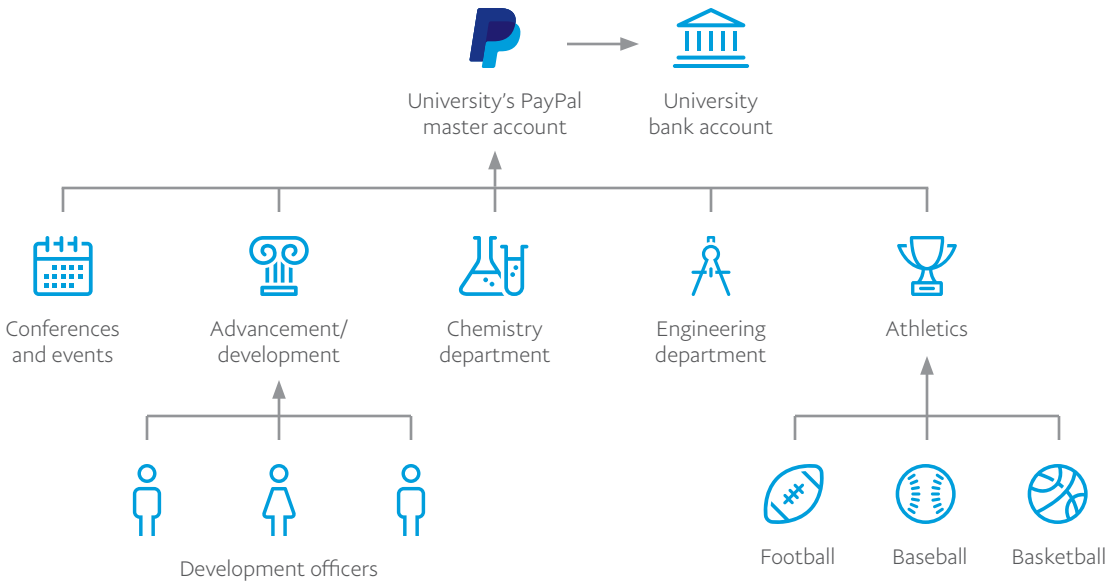
PayPal's hierarchical account structure can be configured at varying levels, such as parent/child, parent/child/grandchild, and so on. Your campus's central administrative organization can set up account structures that correspond to departmental hierarchies, general ledger account structures, or custom hierarchical relationships needed for business operations.

Campuses should look for ways to limit scope so they can reduce the cost of ongoing compliance – for example, eliminating or reducing the storage, processing, or transmission of cardholder data.

Administrators can design the payment process flow to meet business and banking requirements. When establishing the payment process flow, administrators should consider the following rules:

- Payments flow directly into each child account.
- Net balances from each child account can be automatically transferred to the parent account.
- Money from the parent account can be automatically transferred to the institution's bank account on a nightly basis.
- PayPal accounts can be linked to a bank account at any level in the hierarchy.
- Child accounts have access to detailed reporting and research at the transaction level.
- Summary settlement reports are available at the parent account level, enabling central administrators to monitor transaction activity across the payment platform.

This diagram shows how you can configure the PayPal hierarchical account structure:



How PayPal solutions can help limit compliance scope.

Colleges and universities must confirm the scope of their CDE and attest to their PCI DSS compliance annually. Since the cost of achieving and maintaining PCI DSS compliance directly relates to the scope of an institution's CDE, campuses should look for ways to limit scope so they can reduce the cost of ongoing compliance.

In some cases, colleges can reduce scope by eliminating or reducing the storage, processing, or transmission of cardholder data via the institution's networks and system components. PayPal offers several payment services that can help campuses reduce CDE scope, as the following scenarios show.

SCENARIO 1: ELIMINATE PAPER-BASED PROCESSES WITHOUT INCREASING PCI DSS COMPLIANCE SCOPE.

A student group collects funds for group memberships, events, and memorabilia sales. In addition to collecting cash and checks for these items, the group wants to accept credit card payments. However, the amount of revenue generated is not high enough to justify the expense of obtaining a merchant ID and payment terminal.

Therefore, the group processes credit card payments via a paper-based method. The group collects credit card account information on paper forms, and the forms are transferred to a centralized cashiering office for processing. The paper-based process is in scope for PCI DSS compliance purposes, which means student groups or departments using this process must implement all applicable PCI DSS requirements.[7]

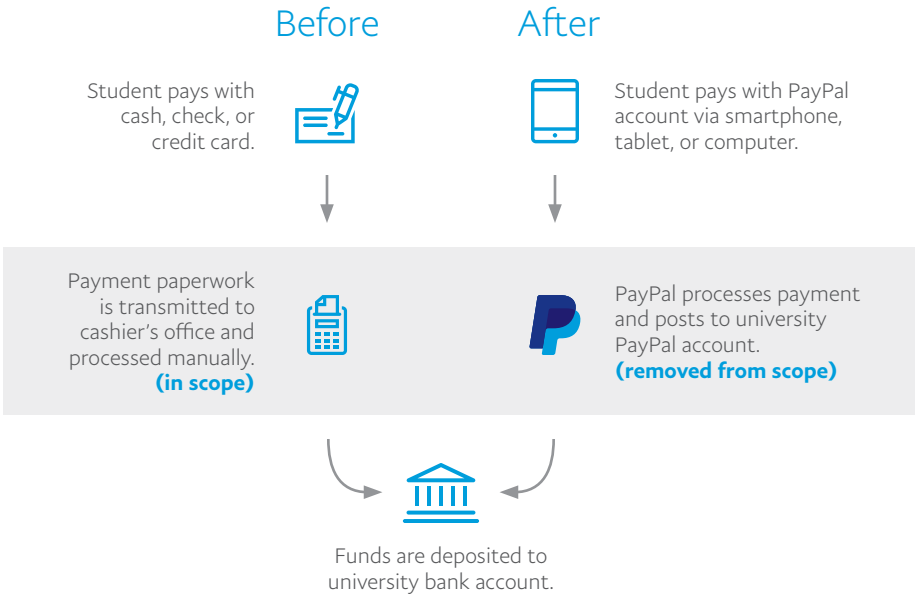
Other campus scenarios in which paper-based processes may be used include the following situations:

- Accepting payments at the door for event registration.
- Selling books, clothing, or other products at events.
- Accepting payments in classrooms for course materials.

The PayPal solution.

The student group or department can offer PayPal and eliminate paper-based processes. Students can use their smartphones, tablets, or computers to pay using their PayPal accounts. The transactions are logged to the student group or departmental PayPal account for reconciliation and reporting. These transactions don't require a campus website or a merchant ID for processing.

Benefit: PayPal removes the paper-based process from the institution's PCI DSS compliance scope.



PayPal solutions can help you manage risk and compliance, while providing the flexibility to support the complexities of credit card payment processing in a campus environment.

7 Including, but not limited to, PCI DSS Requirements 9.5 – 9.8, 12.1, and 12.6.

SCENARIO 2: REDUCE SCOPE BY ELIMINATING THE HANDLING OF PAYMENT CARD DATA.

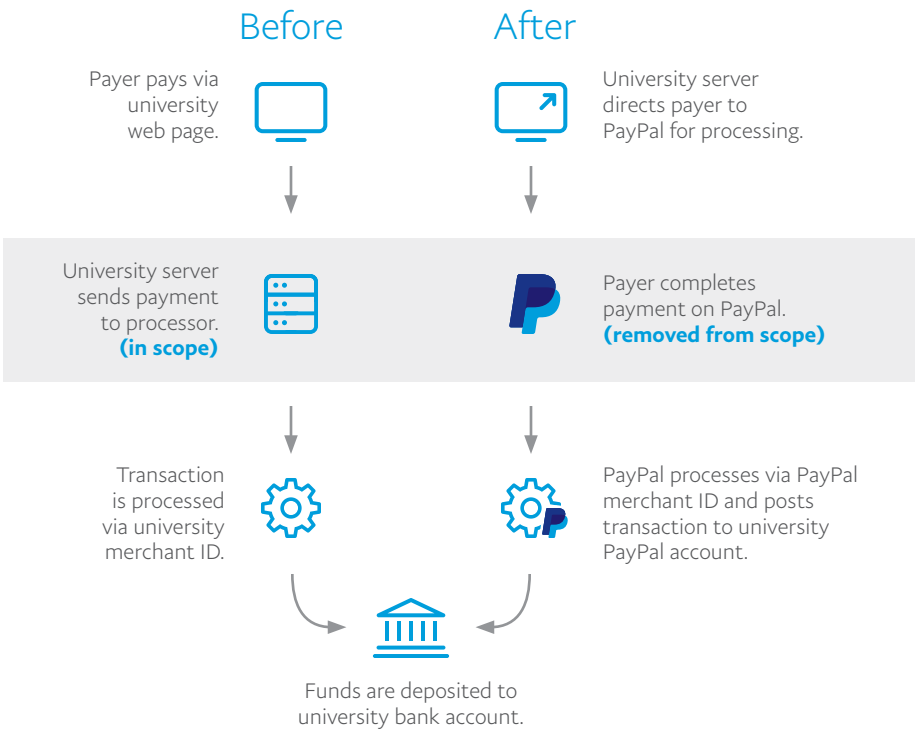
A campus library processes credit card payment transactions – for example, to process late fees or costs for using printers or copiers. Therefore, the website and all the processes related to it are in scope for PCI DSS compliance purposes. The higher education institution has to implement all PCI DSS compliance controls for the payment acceptance method.

The institution has to report on PCI DSS compliance to its acquirer annually. This involves determining the appropriate SAQ type,[8] answering the SAQ, and submitting the SAQ to the acquirer.

The PayPal solution.

The campus merchant can use PayPal to handle online credit card or PayPal payments. The payer is redirected from the campus merchant website to PayPal and can use a debit card, credit card, or PayPal account to complete the transaction. PayPal processes the payment for the university and settles the funds into the university's PayPal account.

Benefit: By eliminating the institution's handling of payment card data, PayPal can help reduce PCI DSS scope – and may help the institution reduce the costs of obtaining and managing merchant IDs.



Reducing the scope of the cardholder data environment not only reduces the risk of a data breach, but it can also reduce the staff and equipment necessary for maintaining PCI DSS compliance.

8 Institutions that are unable to determine which SAQ is applicable for a specific acceptance method should ask their acquirer to verify their PCI DSS validation requirements.

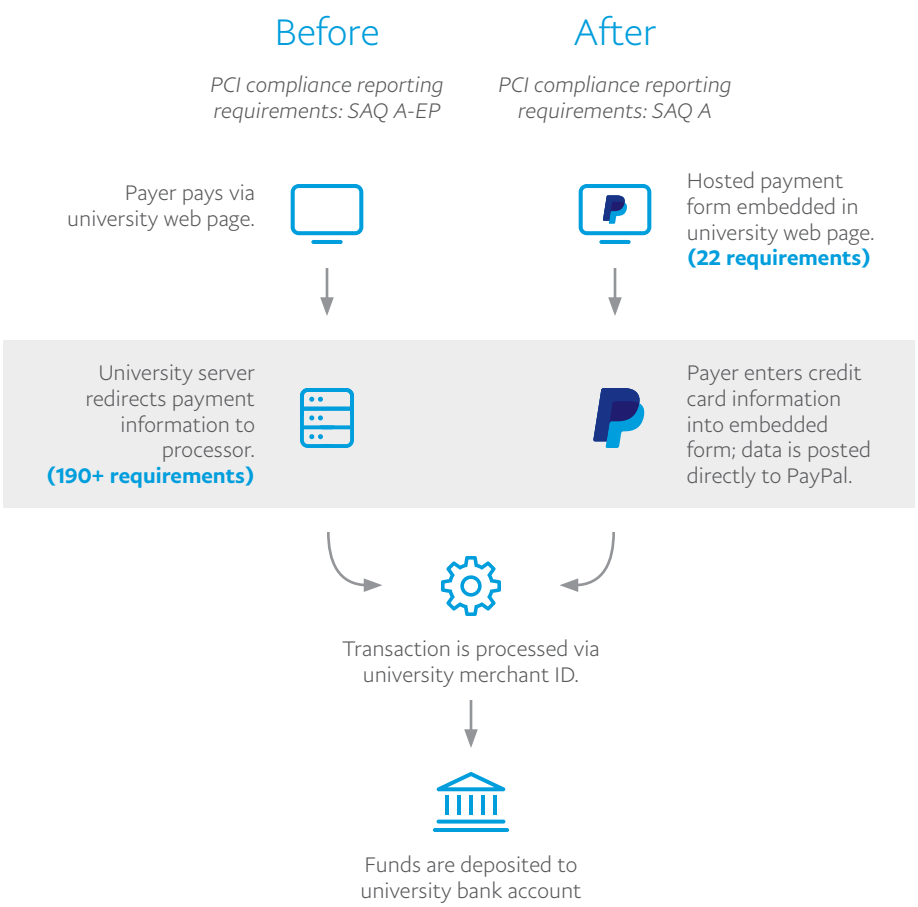
SCENARIO 3: REDUCE THE PCI DSS COMPLIANCE SCOPE OF AN EXISTING ELECTRONIC PAYMENT PROCESS.

A campus organization selling event tickets accepts credit card payment information and processes the payments via an institution's merchant ID. This process is in scope for PCI DSS compliance and requires annual compliance reporting. If the website itself presents elements of the payment page but does not receive cardholder data directly, the PCI DSS requirements that must be in place for this process are, in most cases, defined in SAQ A-EP, which has more than 190 requirements.[9]

The PayPal solution.

The institution can implement PayPal's hosted fields solution, which uses inline frames (iframes) to embed PayPal-hosted payment fields within the campus merchant's web pages. In effect, this process embeds a PayPal web page into the campus web page. When the payer enters payment information into the hosted payment fields and submits the data, the form posts the data directly to PayPal – without involving the systems of the campus merchant or institution.

Benefit: When implemented as instructed by PayPal, colleges and universities can reduce PCI DSS-compliance reporting requirements for this acceptance method to those defined in SAQ A, which contains only 22 requirements.[9]



PayPal allows your institution to offer payment choices that fit campus business needs, while also limiting or reducing PCI DSS compliance scope.

9 *Self-Assessment Questionnaire A-EP and Attestation of Compliance*, PCI Security Standards Council, p. iii: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A_EP.pdf.

Learn more about PayPal for higher education.

You face many challenges when providing secure and compliant credit card payment solutions to campus merchants – and PayPal offers services and products that address these challenges. PayPal solutions can help you manage risk and compliance, while providing the flexibility to support the complexities of credit card payment processing in a campus environment.

For more information about how PayPal can provide seamless solutions within the framework of your college or university, email paypalforhighered@paypal.com or visit paypal.com/highered.

About PayPal.

Founded in 1998, PayPal continues to be at the forefront of the digital payments revolution. PayPal gives people better ways to manage and move their money, offering them choice and flexibility in how they are able to send money, pay, or get paid. We operate an open, secure, and technology-agnostic payments platform that businesses and nonprofit organizations use to securely transact with their customers online, in person, and increasingly on mobile devices.

In 2015, 28% of the 4.9 billion payments we processed were made on a mobile device. With our 188 million active customer accounts, PayPal is a truly global payments platform that is available to people in more than 202 countries, allowing customers to get paid in more than 100 currencies, withdraw funds to their bank accounts in 56 currencies, and hold balances in their PayPal accounts in 25 currencies.

About Sikich LLP.

Sikich is a leading professional services firm specializing in accounting, technology, investment banking and advisory services. Sikich's security and compliance division is dedicated to assisting clients with information security consulting, fraud management, risk mitigation and vulnerability detection and prevention. As a company with an international presence, Sikich has the privilege of working with leading payment card, financial, restaurant, hospitality, health care, nonprofit, government and education organizations from around the world.

Sikich is a Payment Card Industry (PCI) Qualified Security Assessor (QSA), a Payment Application Qualified Security Assessor (PA-QSA), a Point-to-Point Encryption (P2PE) QSA and PA-QSA, an Approved Scanning Vendor (ASV) and a PCI Forensic Investigator (PFI). We validate the full range of Level 1-2 service providers and Level 1-4 merchants against the PCI Data Security Standard (PCI DSS), as well as validating payment applications against the Payment Card Industry Payment Application Data Security Standard (PA-DSS).

The content of this document was developed in conjunction with Sikich LLP, a Qualified Security Assessor.