PCI-EZ

Better security. Less paperwork.

touchnet®

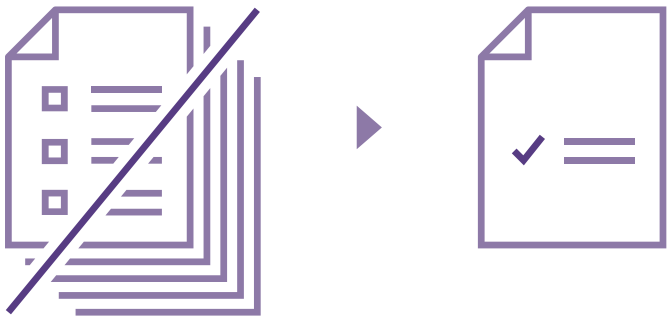
Introduction

The Payment Card Industry (PCI), or more accurately, the Payment Card Industry Security Standards Council (PCI SSC), has been active for more than a decade now. PCI standards define the rules by which all merchants that accept credit or debit card payments must protect cardholder data. Compliance is not optional. It is a responsibility that merchants cannot dismiss or transfer to someone else. Furthermore, failure to achieve compliance can be very costly. That much is pretty well understood by most campus merchants.

Something else that is understood is that PCI compliance is hard to achieve. Standards continually get more complex and difficult. What's more, the effort required to attest your compliance is also escalating. At one time, only larger merchants needed to worry about submitting compliance paperwork. **Now the card brands are requiring that all merchants, even smaller merchants, complete and submit annual compliance documentation.**

The purpose of this booklet is to provide you with information about a sensible approach to managing that ever-increasing overhead of PCI compliance. It is a program we call TouchNet PCI-EZ. PCI-EZ lets you maximize your cardholder data safeguards while you minimize the associated overhead of compliance paperwork at the same time.

Reduce Your PCI Paperwork



ABOUT TOUCHNET

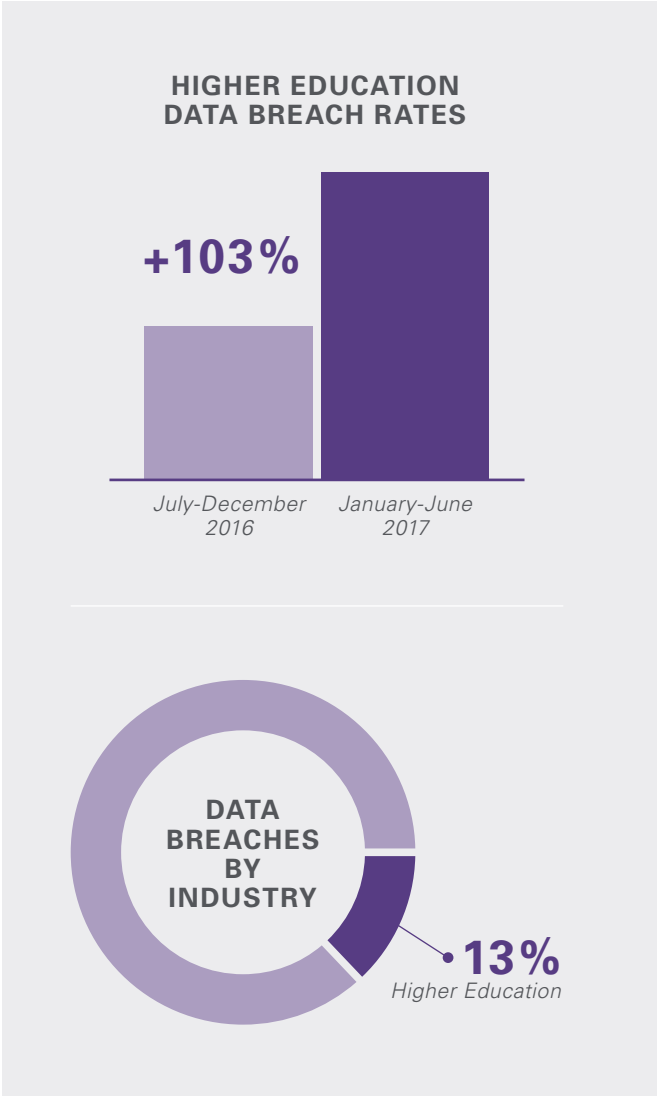
TouchNet is the leading provider of integrated, comprehensive and secure commerce and credentials solutions for colleges and universities. Institutions of higher education rely on TouchNet to unify and secure payments, permissions and other related business transactions campuswide. TouchNet's unmatched integration, transparency and security give institutions greater control over transactions, costs and compliance while providing greater operational efficiencies and self-service access to real-time information. TouchNet is part of the Global Payments (GPN) network of companies and has been serving Higher Education for more than 25 years.

Complexities of Compliance in Higher Education

Campus Data Security Is a Tough Job

Data security is a tough job on college and university campuses. Why? The campus is a complex ecosystem to secure. Colleges and universities are like small cities that contain a wide variety of merchants, many using highly specialized systems. **Data breaches in Higher Education more than doubled during the first half of 2017 compared to the last half of 2016, Gemalto reports*.** There were 118 successful attacks on educational institutions, which accounted for 13 percent of all data breaches in all industries. The report indicated identity theft was the leading motivation for the breaches. So, it's no surprise that Higher Education, with its large number of users, is a highly attractive target for hackers.

Higher Education's challenge is to acknowledge being a high-profile target while managing multiple merchants in a large, diverse payments ecosystem comprising multiple payment points, payment methods and payment channels. Typical retailers – both large and small – operate in a much more uniform environment and therefore can deploy a more streamlined approach to payment security and compliance. Data security on campus is a much more difficult challenge.

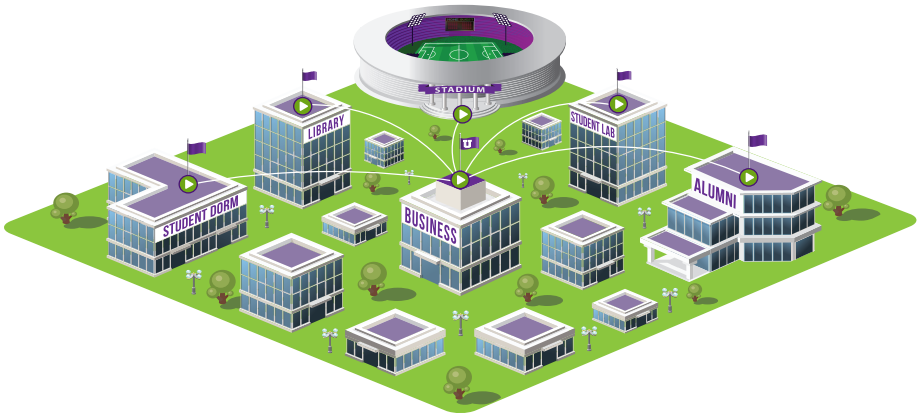


*Source: https://campustechnology.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx

Multiple Payment Points

The typical campus contains many merchants. Any merchant may accept payments using multiple applications from varied locations. Pay points abound, and each must be accounted for by your PCI security plan. Think of all of the departments, organizations, clubs and other areas that may have a need to take payments, either continually or just occasionally.

Campuswide Payments



Then think about the multitude of software and hardware vendors serving these various payment needs and the variety of payment systems involved. Then consider that a data breach in any of these systems is reflected as a breach by your school's brand!

Multiple Payment Methods

Campus merchants also manage a variety of payment options to meet expectations and competition for revenue.

CREDIT/DEBIT CARDS

Payment cards are the most common payment method in use. Credit and debit cards can be classified as either magnetic stripe or chip cards.

AUTOMATED CLEARING HOUSE (ACH)/ECHECKS

Automated Clearing House (ACH) is a payment method tied directly to a student's bank account. It can also be used to disburse financial aid credit balances to students.

WIRES

Most often used in cross-border payments, wires are an important payment method to institutions working to attract international students.

CAMPUS CARDS

Campus ID cards are closed-loop payment cards that work only for campus-authorized purchases and are tied specifically to a campus student account.

Multiple Payment Channels

Payments arrive on (and leave from) the campus through multiple channels. At one time, payments were primarily either made at a cashier's window or mailed to the campus business office. Now, of course, to meet the expectations of students, parents, alumni and others in the community, campuses must accommodate a variety of additional credit/debit card-payment channels.

ECOMMERCE (ECOMM)

ECommerce payments are those made online via internet applications. These are referred to as card-not-present transactions.

POINT-OF-SALE (POS)

POS payments are in-person payments made at the point-of-sale. These are assisted payments at a cashiering point-of-sale device and are referred to as card-present transactions.

MOBILE POINT-OF-SALE (MPOS)

These are also POS payments. They are in-person payments made with a cashier's assistance using a portable, handheld device to accept and transmit the payment information.

MOBILE PAYMENTS (EWALLETS)

Mobile payments are transactions made using smartphones as "payphones." Mobile payments are an emerging payment channel for facilitating transactions using the consumer's smartphone and an electronic wallet app (eWallet). Mobile payments can be initiated either online or at the point of sale; the smartphone eWallet interacts with the computer or POS device to conduct a real-time payment. Mobile payments depend upon newer technologies like near-field communications (NFC).

The Trend toward Omnichannel Experiences

Adding to the complexities of campus commerce are the growing student expectations for omnichannel experiences on campus. As a major contributor to student satisfaction, many campuses are working to develop a consistent experience across all the payment channels, whether online, in person or mobile. **However, for payments, omnichannel should extend beyond simply a consistent user experience.** True omnichannel payments also require a back-end process streamlined so that all payment options are also processed and protected in the same fashion and with the same vigor. Campuses can waste significant time and money by trying to stitch together many disparate solutions to handle different payment sources.

Choosing the Right Self-Assessment Questionnaires (SAQs)

If you are eligible to self-assess your PCI compliance, you will need to determine which SAQ to submit for each unique combination of merchant, payment point and payment method. The type and number of questions included in each SAQ and the need for periodic vulnerability and penetration tests are dependent upon details of the specific payment infrastructure being evaluated. Once submitted, these self-attestations are reviewed by your Acquirer.

PCI Self-Assessment Questionnaires

SAQ	DESCRIPTION	QUESTIONS	VULNERABILITY SCAN	PENETRATION TEST
A	Fully Outsourced eCommerce • Card not present • Entirely outsourced • All elements of all payment pages delivered by service provider	22	N	N
A-EP	Partially Outsourced eCommerce • Ecommerce transactions • Processing entirely outsourced • Merchant control of eCommerce website related to how consumers' card data is transmitted to service provider	191	Y	Y
B	Card Swipe (Dial-up), Imprint • Imprint machine and/or stand-alone, dial-out terminal	41	N	N
B-IP	Card Swipe (Internet Connected) • Uses only stand-alone, PTS-approved point-of-interaction (POI) devices connected via IP to your payment processor	82	Y	N
C-VT	Web-based Virtual Terminal • Virtual payment terminal accessed by an internet-connected web browser • Hosted by a PCI DSS-validated third-party service provider • Does not have any attached hardware devices	79	N	N
C	Payment Application (Internet Connected) • Payment application system and an internet connection on the same device and/or same local area network (LAN)	160	Y	N
D	All other SAQ-eligible merchants	329	Y	Y
P2PE	PCI-Listed P2PE Solution	33 (-2)	N	N

SAQs

Don't let the name "Self-Assessment" lead you to believe that SAQs are not difficult. In fact, completing SAQs is challenging and confusing and often requires assistance from consultants to help understand what is being asked and how to meet the specifics of each requirement.

The TouchNet PCI-EZ Program

Better Security AND Less Paperwork

Most merchants understand that PCI compliance is a responsibility they cannot dismiss, and failure to achieve compliance can be very costly. But PCI compliance is difficult. Standards continually get more complex and the annual effort needed to attest compliance has escalated, too. **The TouchNet PCI-EZ program is a sensible approach to managing that ever-increasing overhead of PCI compliance.** It helps campuses limit their overall PCI scope while also reducing the load of annual documentation that accompanies today's PCI efforts. PCI-EZ and its underlying software, equipment and services reduce institutional risk, lower overhead, enhance manageability and increase operational efficiencies. In other words, PCI-EZ maximizes cardholder data safeguards while, at the same time, minimizing the associated overhead of compliance paperwork.

UNIQUE RESULTS FROM A UNIQUE PARTNERSHIP

TouchNet is able to offer the PCI-EZ program because of our unique relationship with Heartland Payment Systems, our sister company under the Global Payments umbrella. TouchNet plays the role of a merchant service provider to your institution, providing onboarding, support services and the technology platform for campuswide processing. Heartland serves as the Merchant Acquirer and is ultimately responsible for your PCI compliance. Because of our close working relationship, Heartland compliance teams have an intimate knowledge of the TouchNet Certified DataCenter, our products and services and our overall merchant processing environment. This allows TouchNet and Heartland to integrate policies and procedures to streamline PCI compliance for our customers.

globalpayments

touchnet® Heartland

Three EZ Steps to a Strong PCI Foundation

1 IMPLEMENT FULLY CERTIFIED TECHNOLOGY

The right technology starts with the right payment platform. TouchNet U.Commerce is the ideal solution. It is not only fully PCI compliant (compliant with the requirements of PCI DSS, PA-DSS, PTS and P2PE) and Europay-MasterCard-Visa (EMV) certified, but also provides your campus with the flexibility and scalability to support multiple payment methods, payment channels and payment locations. U.Commerce offers important technical considerations for your choice of platform.

Centralized Control and Management

This is the ability to manage users, reporting and compliance through a single platform. The more merchants you have processing payments through one centralized platform, the smaller your PCI footprint becomes. This means less time auditing and reviewing payment applications, payment terminals and vendor relationships, and ultimately less paperwork for you.

Support for a Link-Out Payment Strategy

Your campus should have support for a link-out payment strategy for third-party campus partners accepting payments within their products. For example, your campus parking solution should be able to link into your centralized, PCI-compliant payment platform to enable payment card acceptance.

Secure Protocols for Transmitting Payment Card Data

Since June 30, 2018, Secure Sockets Layer (SSL) and early versions of Transfer Layer Security (TLS) are no longer considered PCI compliant. All merchants and service providers processing payments are required to be on TLS 1.1, but the PCI Council is strongly encouraging the adoption of TLS 1.2 protocol.

Reducing Fraud at the Point of Sale

The reduced potential for card fraud is the first benefit of deploying EMV-compliant devices in your POS environment. EMV greatly reduces the likelihood of card fraud by making it difficult to duplicate cards physically. Another important benefit is the ability to accept contactless payments through EMV-enabled POS terminals and smartphone eWallets. But EMV alone is not enough to protect all cardholder information because it does not protect data in motion. Point-to-point encryption (P2PE) is needed to do that. The combination of EMV and P2PE is so effective, the card brands offer incentives to encourage all merchants to invest in those technologies.

2 TRANSACT WITH TOUCHNET + HEARTLAND

Your Merchant Services Acquirer (MSA) is the arbiter of your PCI compliance efforts, so the TouchNet + Heartland partnership is the most important relationship concerning your PCI compliance. As your Acquirer, TouchNet + Heartland works with the card brands to ensure your campus meets the compliance standards established by the PCI Council. It is the Acquirer's duty to define each merchant's level, the SAQs required for compliance validation and acceptable payment system controls.

It's important to view your Acquirer as a strategic choice rather than as a choice of the lowest-cost vendor available for your processing services. When viewed this way, your goal becomes to provide your Acquirer with full knowledge and understanding of how your transactions flow and the payment technology stack handling those transactions on campus. This way, the vast majority of typical SAQ questions can be predetermined and answered without you, the merchant, doing the legwork.

When your MSA understands your entire payments environment, you can save time and effort by asking your MSA to help you eliminate redundant and unnecessary documentation and determine answers to many SAQ questions in advance, significantly reducing the number of questions you have to directly answer each reporting cycle. Your MSA can help you organize the number of campus Merchant IDs (MIDs) for which you report compliance, further reducing your annual reporting. Finally, as your partner, your MSA can recommend incentive programs for adopting payment technologies such as EMV and certified P2PE (point-to-point encryption) that can eliminate the requirement to submit some SAQs entirely.

SAQ SUBMISSION PROCESS

MERCHANT
Submits SAQs to Acquirer

ACQUIRER
Acquirer reviews and submits to card brands

CARD BRANDS
Validates merchant compliance

3 ORGANIZE YOUR MERCHANT STRUCTURE

Limit Your Cardholder Data Environment (CDE)

PCI compliance begins with knowing your PCI scope, or "footprint." That is, you must identify everywhere cardholder data might be processed, stored or transmitted. In addition, you must define all merchants on campus involved in processing payments throughout the year as well as their payment types, channels, methods and locations. The result is called your cardholder data environment (CDE). **Each unique combination of merchant, payment channel and service provider connectivity within the CDE requires annual submission of its own function-specific SAQ.** Acquirers review and approve each merchant's SAQs for applicability and accuracy and are responsible to the card brands for your compliance. Obviously, reducing your CDE (i.e., reducing your PCI footprint) is a critical step to reducing your overall PCI efforts.

Your CDE seems like it should be a fairly static environment. Many times, however, we find that campus merchants come and go within the year for special events or activities, so it's important to recognize these pop-up merchants. These "rogue payment points" are the enemy of compliance and security. PCI is 12 years old, and this problem has been at the top of the list since the beginning. Your CDE documentation should clearly identify short-term payment points and should be quickly available if your compliance is questioned or a breach occurs.

Manage Your Merchant Identification Numbers (MIDs)

More is not necessarily better when it comes to the number of merchant identification accounts (MIDs) on campuses. Not long ago, Level 4 merchants could work closely with their Acquirer and forego submitting most annual paperwork. So, many campuses defined multiple merchant IDs to avoid the volume criteria of higher levels and therefore reduce the amount of onerous paperwork required. That doesn't apply today. All merchants must report their PCI compliance annually. Additionally, many campuses define multiple IDs for the reporting benefits they find in separating reconciliation statements by ID. TouchNet solutions answer that challenge by providing that same convenience in reporting and reconciliation without the need for multiple MIDs on campus. Reducing the count of MIDs on campus lowers your overall PCI paperwork requirements.

PCI-EZ in Action

PCI-EZ for eCommerce

PCI FOOTPRINT REDUCTION

PCI-EZ eCommerce features are based upon the underlying TouchNet U.Commerce technology. One of the biggest PCI benefits available from the U.Commerce platform is support for "link-in/link-out" payment processing. This ability lets campuswide vendors of specialized business applications use the TouchNet platform to process their payment transactions, effectively removing their software from the institution's CDE and reducing its PCI footprint. **This eliminates the need for PCI compliance reporting for all business systems that take advantage of this opportunity.** These systems are effectively reclassified as business software, not merchant systems, and are considered out of PCI scope.

PA-DSS COMPLIANT PAYMENT APPLICATION

Each release of TouchNet U.Commerce software is reviewed for compliance with the Payment Application – Data Security Standard (PA-DSS). This review is performed by an independent third-party payment application assessor. Once the products are certified as compliant, they are listed on the PCI SSC website as "Validated Payment Applications."

PCI DSS COMPLIANT DATACENTER

In addition to compliance with payment application standards, the TouchNet platform is hosted in the TouchNet Secure DataCenter. The TouchNet DataCenter and its procedures and processes are reviewed annually for compliance with the Payment Card Industry Data Security Standard (PCI DSS). This review, too, is performed by independent, third-party auditors.

SMART SAQs

PCI-EZ provides another unique service for eCommerce merchants – Smart SAQs. Smart SAQs are built using information provided by TouchNet and Heartland to our partner, ControlScan, during annual software and compliance reviews. PCI-relevant information is stored for each TouchNet U.Commerce solution, allowing TouchNet customers to simply select a TouchNet product to receive a pre-filled-out SAQ for that specific product and merchant type (e.g., SAQ A for Bill+Payment customers). The pre-answered questions address TouchNet product-specific security features and our PCI-compliant DataCenter environment. Questions remaining for the merchant to answer include topics such as campus policies and procedures and physical security processes.

PCI-EZ for Point of Sale (POS)

EMV AND P2PE PROTECTIONS

In addition to those benefits afforded eCommerce merchants, TouchNet PCI-EZ delivers added features to merchants with point-of-sale (POS) environments. More than just paperwork reduction, **PCI-EZ can eliminate some PCI paperwork entirely.** First, PCI-EZ is based upon use of EMV-compliant card equipment. Then, PCI-EZ includes a PCI-validated P2PE solution for qualifying POS devices. Implementation of a PCI-validated P2PE solution helps protect cardholder data "in motion" from the point of interaction (POI) to the payment processor. This is called point-to-point encryption, or just P2PE. Because PCI-EZ offers you P2PE protection for cardholder data, you effectively eliminate your local computers and campus network from your PCI scope and qualify for a shortened SAQ P2PE questionnaire.

Eliminate POS Paperwork

SOFTWARE
TouchNet Payment Center

HARDWARE
Validated P2PE

PROCESSING
TouchNet Transaction Services

DESCRIPTION	SAQ	QUESTIONS
Payment Center + Nonvalidated Hardware	C	160
Payment Center + Validated P2PE Hardware	P2PE	33
Payment Center + Validated P2PE + Transaction Services	N/A	0

Elimination of Some SAQs Entirely

Merchants processing POS transactions using qualifying TouchNet technology automatically are enrolled in applicable exemption programs offered by the card brands. These special programs, such as Visa's Technology Innovation Program (TIP), reward merchants for investing in security technology. They completely eliminate the need to submit SAQs on an annual basis for qualifying POS environments. These exemption programs have basic qualifications above and beyond the use of TouchNet and Heartland. Those include:

1. **Merchant must be PCI compliant.**
2. **Seventy-five percent or more of the merchant's card-present transactions must be processed through EMV devices supporting both contact and contactless EMV.**
3. **The merchant has not experienced a breach within the past 12 months.**
4. **The merchant does not store sensitive authentication data, such as card account numbers, the card verification value or PINs.**

Once this information is verified and qualifying MIDs are enrolled in the exemption program, you will no longer be required to submit PCI paperwork for these MIDs. Any MIDs for point-of-sale devices outside the TouchNet environment may also be eligible for the exemption program. Those that are not eligible may still report compliance through the self-service portal provided as part of the PCI-EZ program.

PCI-EZ for Required PCI Testing

This close working environment also means that PCI-EZ can include security services through a partnership with ControlScan. ControlScan is a PCI-certified Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). ControlScan services include access to a self-service portal for TouchNet merchants to validate compliance, review periodic vulnerability scans and discuss PCI-security issues with live customer service representatives. External vulnerability scans are required to verify that a merchant's networks adhere to the guidelines of PCI DSS Requirement 11.2.2. To be acceptable, these scans must be conducted by a PCI ASV. An ASV is an organization with a set of security services and tools to conduct external vulnerability scans certified by the PCI Council.

Conclusion

PCI-EZ offers colleges and universities a path to protecting sensitive payment data and achieving PCI compliance, while simultaneously reducing the annual overhead involved in compliance documentation. PCI-EZ is not magic, however. It represents the benefits of putting the right software, hardware and services from the right partners together in a rational approach to deploying a comprehensive and secure payment system.

PCI-EZ is possible because of the unique relationship between TouchNet and Heartland Payment Systems (both Global Payments companies). The result is a detailed understanding and deep trust in the resulting merchant transaction environment for your Acquirer, the arbiter of your PCI compliance success. This, in turn, makes known key elements of the payment process so that many of the critical questions to which a PCI SAQ response is required can be predetermined. But more than simply knowing answers to questions in advance or qualifying for shortened forms, PCI-EZ can eliminate some PCI paperwork entirely for the merchant's POS environment, all while enhancing the overall level of data protection.

THE BOTTOM LINE IS THIS:
The PCI-EZ program and its underlying software, hardware and services reduce institutional risk, lower overhead, enhance manageability and increase operational efficiencies. These are desirable results aggressively sought by most campuses and are the benefits of unified campus commerce.

Appendix: PCI Rules and Regulations

Payment Compliance

There are a lot of rules to follow when you are in the business of accepting card payments. Most come from PCI, but there is also a long list of operating rules that come directly from the card brands. You agree to all of them when you sign a standard merchant agreement – which you must do to take payments.

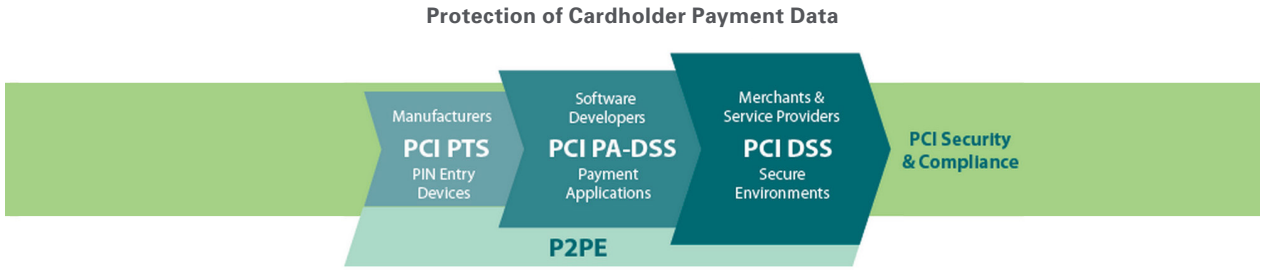
In fact, if you remember nothing else from this guide, remember that every merchant that accepts Visa, MasterCard, American Express, Discover or other card transactions must be PCI-compliant. This obligation is clearly stated in every merchant processing agreement and the operating rules of the major card brands. Yes, there are a few exceptions for very small retailers without a physical presence, but these are generally not available to college and university merchants. PCI compliance is a reality of doing business in the digital age, and the best strategy is to embrace the requirements and make them a routine part of your business operations.

THE PAYMENT CARD INDUSTRY COUNCIL

The Payment Card Industry Security Standards Council (PCI SSC) is an organization of card brands that was created for the "ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection." These standards can be a confusing array of requirements and paperwork to many merchants. Yet, data thieves have become more determined and sophisticated in their attacks on payment transactions, so standards must continue to evolve in order to keep pace.

For merchants on campus, there are four primary standards to understand, a fifth standard not yet part of the PCI constellation, and other numerous "guidelines," such as the guideline for cloud computing. All pertain to safeguarding cardholder data for credit or debit card payments. The PCI SSC, however, does not have the final say in whether or not you are in compliance, or even if you are correctly reporting your compliance status. That remains with your Merchant Services Acquirer and ultimately the card brands (Visa, MasterCard, etc.).

Payment Card Industry Security Standards



Ecosystem of payment devices, applications, infrastruture and users

Source: PCI Security Standards Council

Cardholder Data Security Standards

Today's merchants face a confusing array of payment requirements, both from the PCI SSC and also from the major card brands directly. The interesting thing about payment data security is there are actual and tangible specifications to be met. This is unlike other security laws, such as the Gramm-Leach-Bliley Act (GLBA) or the Family Educational Rights and Privacy Act (FERPA) in Higher Education. Neither of these has tasks that must be performed and results that must be annually attested, but campuses can be challenged in court to prove compliance. Here is a brief overview of each of the important standards you need to be familiar.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

This standard applies to all entities that store, process or transmit cardholder data, covering the technical and operational components of a merchant's payment systems – the processes and environments through which payments are accepted. The requirements of the PCI DSS are organized around a set of 12 basic principles. (See table below.)

All campus merchants that accept card payments must comply with PCI DSS requirements. It's that simple. What's not so simple is the identification of all the merchants, payment systems and payment points active throughout the campus landscape and assessing the PCI compliance of each unique combination. While merchants are responsible for achieving compliance, it is each merchant's Acquirer that assigns merchant levels, oversees compliance results and defines the rigors of PCI DSS compliance reporting.

PCI DSS Basic Principles

BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
PROTECT CARDHOLDER DATA	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
IMPLEMENT STRONG ACCESS CONTROLS	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
REGULARLY MONITOR AND TEST NETWORKS	10 Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
MAINTAIN AN INFORMATION SECURITY POLICY	12. Maintain a policy that addresses information security for all personnel

PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS)

PA-DSS provides guidelines for protecting cardholder data within software systems that store, process or transmit cardholder data and that are sold, licensed or distributed to third parties. To be compliant, these products must be certified by the PCI Council. The vendors that develop the software are responsible for getting their products certified. Merchants that use the vendor-supplied systems must ensure their vendor's software appears in the list of certified payment applications posted on the PCI Council's website.

PIN TRANSACTION SECURITY STANDARD (PTS)

The PTS standard applies to entities that specify, make or implement hardware PIN-entry devices that process card payments and manage associated personal identification numbers (PINs). Merchants may use only compliant devices tested and approved by the PCI Council. The list of approved devices can be found on the PCI Council's website.

POINT-TO-POINT ENCRYPTION STANDARD (P2PE)

P2PE is a standard for solution providers who build or implement data encryption as part of the effort to protect cardholder and sensitive authentication data "on the move." When merchants use a PCI-validated P2PE solution, their cardholder data is unreadable from the time it is captured until it reaches the secure decryption environment at the merchant bank. This makes the data less desirable to thieves and less valuable if the data is stolen in a breach. These merchants also may have fewer applicable PCI DSS requirements to comply with, helping simplify compliance efforts.

Europay-MasterCard-Visa Standard (EMV)

Administered not by the PCI Council but by EMVCo, this optional standard defines the rules of interoperability and security for the new chip cards (payment cards with an embedded computer chip). Released first in Europe and designed primarily to reduce card fraud, this set of standards also defines how devices and systems interact for newer technologies, such as contactless and mobile payments.

Merchant Levels

Your Merchant Services Acquirer assigns one of four "levels" to campus merchants based upon the volume and type of transactions each merchant generates in a year. (See table at right.) This merchant level dictates how a merchant must go about validating its ongoing compliance with PCI requirements. Level 1 merchants (higher risk) must submit an annual Report on Compliance (ROC) from a third-party Qualified Security Assessor (QSA) or certified internal auditor. Merchants in Levels 2-4 can evaluate and report their own compliance by completing and submitting annual compliance reports called Self-Assessment Questionnaires (SAQs).

Visa's Merchant Levels

LEVEL	DESCRIPTION
1	Any merchant processing greater than 6M Visa transactions per year, any merchant that has suffered an account data compromise, and any other merchant that Visa determines should meet Level 1 requirements.
2	Any merchant processing from 1M to 6M Visa transactions per year.
3	Any merchant processing from 20,000 to 1M eCommerce Visa transactions per year.
4	Any merchant processing fewer than 20,000 eCommerce Visa transactions per year and all other merchants processing up to 1M Visa transactions per year.

Glossary of Terms

ACH .....Automated Clearing House. National banking network for the processing of electronic debits (i.e., electronic checks).

ASV .....Approved Scanning Vendor. Certified technical services provider validated to have the training and tools needed to perform periodic external vulnerability scans for merchants.

CDE .....Cardholder Data Environment. The sum total of all merchant systems, networks, applications, devices, people and operations that touch, store, process or transmit cardholder data.

eCommerce.....The environment for online, card-not-present, electronic payments made via computer payment applications.

EMV.....Europay-MasterCard-Visa Technology Standard. Technical and operational standards for interoperability and security of transactions originating with the new chip cards – payment cards with an embedded computer chip.

EMVCo.....The organization that publishes and maintains EMV standards.

Mobile.....Either eCommerce or POS payments (card-not-present or card-present) originated using a smartphone or tablet app, most often in a contactless, NFC environment.

MPOS.....Mobile Point of Sale. POS card-present payments collected using handheld, portable card devices.

MSA .....Merchant Services Acquirer. Also known as the Acquirer, or payment processor. Recruits merchant's business, processes payment transactions, reviews PCI compliance efforts and validates merchant's annual PCI paperwork.

NFC .....Near-Field Communications. Short-range radio frequency communications between physical or virtual cards, smartphones, tablets, etc. and the card reader to enable contactless transactions.

Omnichannel.....A payment environment of multiple payment methods that exhibits a consistency across all access methods in consumer experience, data security and ease of use.

P2PE.....Point-to-Point Encryption. Protects cardholder data by encrypting data as it enters the POI (point of interaction) device and moves to the payment processor.

PA-DSS .....Payment Application - Data Security Standard. Requirements for payment application software.

PCI DSS.....Payment Card Industry Data Security Standard. Requirements for merchant processes and infrastructure in order to protect cardholder data. Built on 12 basic principles.

PCI-EZ.....TouchNet program that leverages its U.Commerce software systems, Heartland payment processing services and selected EMV-enabled payment devices to provide customers with better PCI compliance and less PCI paperwork.

PCI SSC.....Payment Card Industry Security Standards Council. The organization that publishes and maintains PCI standards.

PIN.....Personal Identification Number. Numerical value that is associated with and enabling processing for certain debit card transactions.

POS .....Point of Sale. The payment environment for in-person, card-present, cashier-assisted payments at the point of interaction.

PTS.....PIN Transaction Standard. Requirements for securing PIN-entry payment devices.

QSA.....Qualified Security Assessor. Security service consultant certified to analyze and assist merchants in PCI compliance activities.

ROC.....Report on Compliance. Documentation submitted annually to validate ongoing PCI compliance in Level 1 merchants and service providers.

SAQ.....Self-Assessment Questionnaire. Documents merchants submit annually to self-attest to their PCI compliance.

TIP.....Technology Innovation Program. A Visa program of merchant incentives to hasten adoption of new technologies, such as EMV and P2PE. Other card brands offer similar programs.

touchnet®

TouchNet Information Systems, Inc.
15520 College Blvd., Lenexa, KS 66219 USA
1.800.869.8329 | +1.913.599.6699
touchnet.com

*A **Global Payments** Company*