

PCI-EZ

Dave Swan, Regional Sales Manager | Touchnet

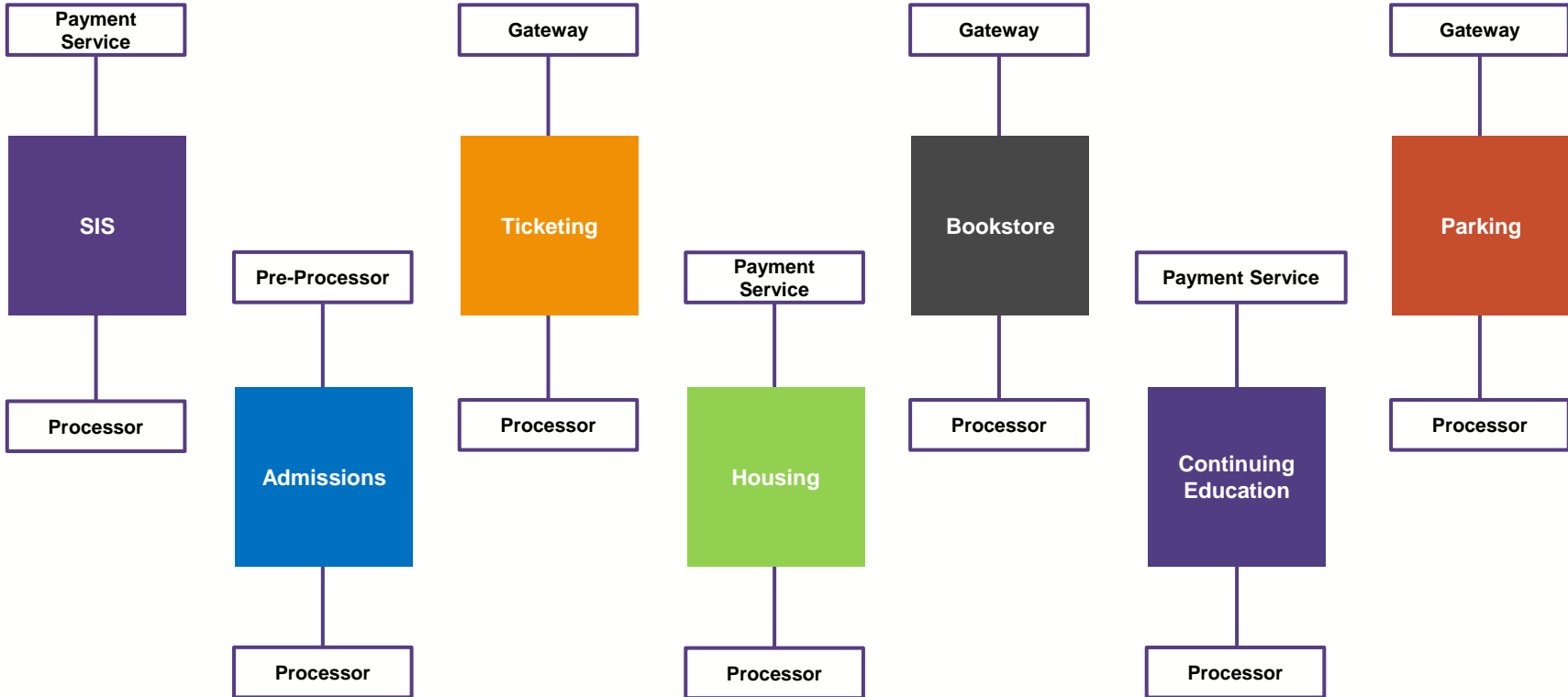
About TouchNet

- Established Kansas City Metro, 1989
- Commerce Platform Provider
- Heartland Payment Systems, 2014
- Global Payments, 2016
- Higher Education Focused
- Software and Service Provider for 1000+ HE Institutions
- Strategic Partnerships: Ellucian & PeopleSoft
- 200+ TouchNet Ready Partners

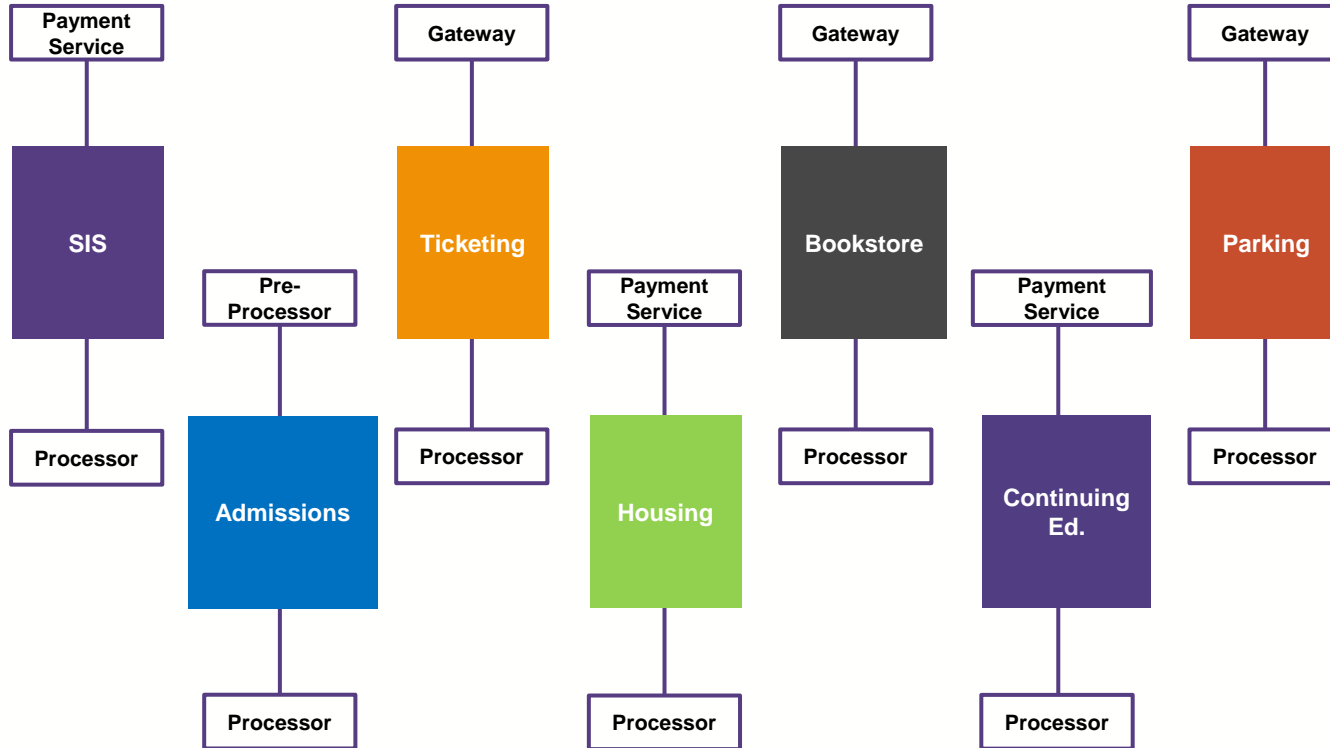
Touchnet's U.Commerce Platform



The Evolution of Payments (on Campus)



Some of the Challenges...



7 x Reconciliations

ERP|Processor|Bank

Vendor Management

Billing Back Merchants:
- Processing Fees?

Posting:
- Interchange
- Revenue
- G/L

PCI Impact
- SAQ's 7 or 1?

7 merchant accts or 1

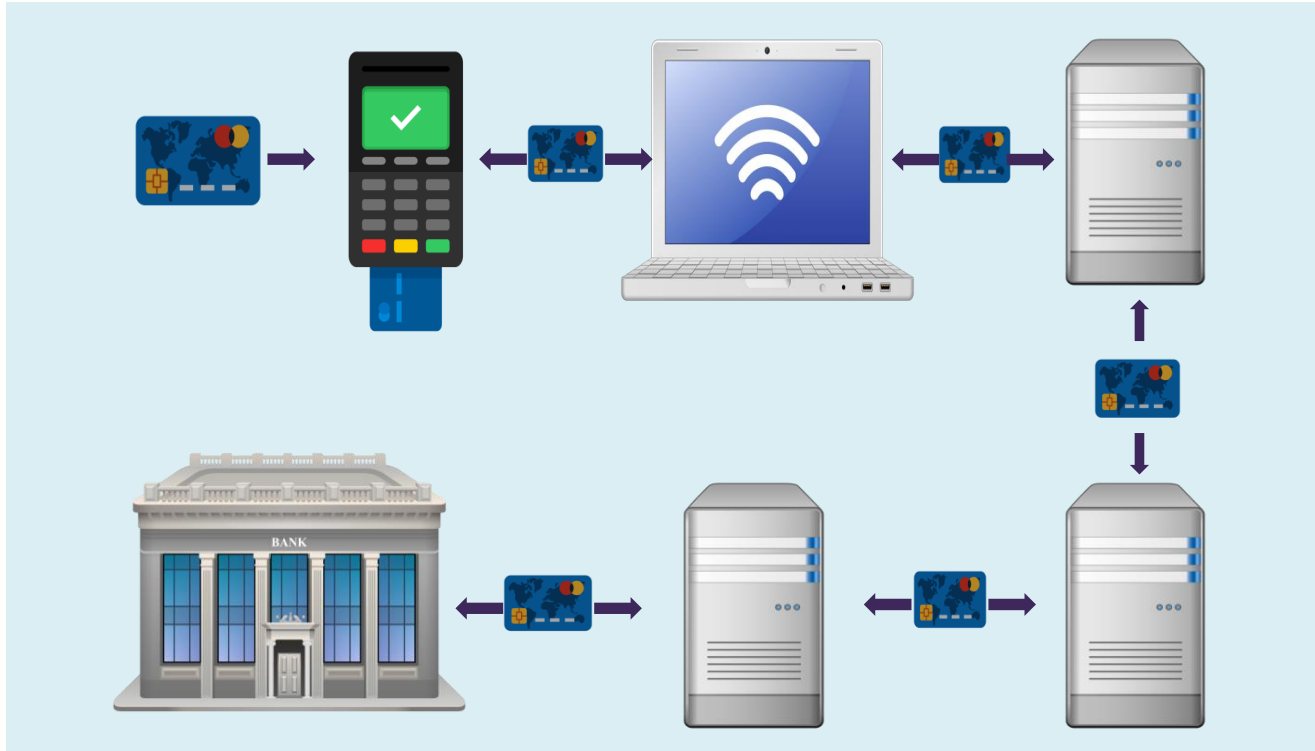
Adding to the Pain, Devices Across Campus



Elite POS

Echo POS

It's more than just the POS device in scope



- POS Devices

+

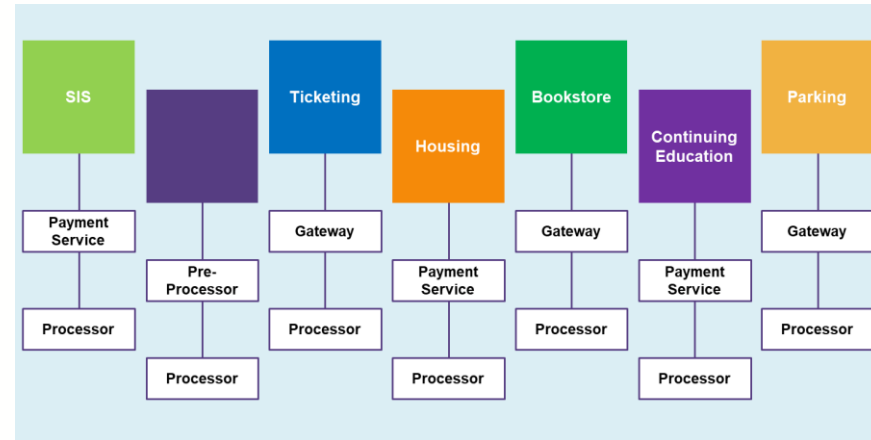
- Network
 - LAN/Wi-Fi
- Terminals/PC's
- Routers
- Servers

Self Assessment Questionnaires (SAQs)

SAQ	Description	#of Questions	Vulnerability Scan	Penetration Test	SSL/TLS Impact
A	Card-not-present merchants (fully outsourced)	22 (+8)	N	N	N
A-EP	Partially outsourced e-commerce website (direct post)	191 (+52)	Y	Y	Y
B	Card swipe (dial-up), Imprint	41 (0)	N	N	N
B-IP	Card swipe (Internet connected)	82 (-1)	Y	N	Y
C-VT	Web-based virtual terminal	79 (+6)	N	N	Y
C	Payment application connected to Internet	160 (+21)	Y	N	Y
D	All other SAQ-Eligible Merchants	329 (+3)	Y	Y	Y
P2PE	PCI-Listed P2PE Solution	33 (-2)	N	N	N

Questions About Your Payment Environment

- How are you taking payments today
 - Online, In-Person, Over the Phone, Mail, other...
- How many points of interaction (POI)
 - How many devices?
- Is there a PCI Team (lead by IT or Business Office)
- Are you PCI compliant today?
- Working with a QSA?
- How many SAQs?
- To whom do you “Attest” your compliance?
- Are you centralized or decentralized?
- Have you established access controls?



Laying the Foundation

PCI-EZ
Better security. Less paperwork.

touchnet



Reader's digest

HA! REALLY DUMB CRIMINALS

FAIL TO JAIL:
Funny Tales of Humbling Bandits
PAGE 28

LEONARD
ERBORN ON
THE ROAD
PAGE 31

NEVER HAVE
BREAST CANCER
Experts consider
PAGE 32

THE GOOD NEWS
ABOUT GLOBAL
WARMING
PAGE 34

THE IMPROVEMENTS OF IRON
LAKESIDE, THE FIRST MEDICINE
DRAMA IN REAL LIFE, NO BIRTH
DESPITE YOUR VICKI ANDERSON NOVA
PAGE 35

THE LEOPARD
A Novel by
PAGE 38

FIGHT FOR A
WORLD FOR
REASON
By
PAGE 32

ADVICE TO A
BOY LONELY
IN MONTREAL
PAGE 36

THE IMPROVEMENTS OF IRON
LAKESIDE, THE FIRST MEDICINE
DRAMA IN REAL LIFE, NO BIRTH
DESPITE YOUR VICKI ANDERSON NOVA
PAGE 35

PCI-EZ
Better security. Less paperwork.

touchnet

Reader's Digest

Three Keys to the PCI-EZ Strategy

1 Platform

2 Acquirer

3 Merchant



PCI-EZ: Key #1

1 Platform



- Scales to Campuswide Payment Initiatives
- Support Payment Methods & Locations
- Security, Compliance & Reporting Controls

2 TRANACT WITH
TOUCHNET + HEARTLAND

3 ORGANIZE YOUR
MERCHANT STRUCTURE



Pick a Platform



Online: Bill+Payment & Marketplace

Student Account Center

My University | Logged in as: Amy L. Student | Logout

My Account | Payment Plans | Deposits | Refunds | Help | My Profile

Welcome to Payment Center!

Make payments, view account activity, store payment profiles, and set up parents or guardians to access your account.

Registration for next semester is final January 23rd and all tuition fees are due by January 18th, and make payments on your account.

You can pay all fees by credit card or electronic check here.

Remember to complete your Residence Hall License Agreement Form with the Residence Life Office.

Account: Amy L. Student ID: ****1234

Balance	\$18,377.43
Estimated Financial Aid	\$1,700.00
Balance Including Estimated Financial Aid	\$16,677.43

[View Activity](#) [Enroll in Payment Plan](#) [Make Payment](#)

My Profile Setup

- Authorized Access
- My Payment Profile
- Electronic Refunds
- Auto Bill Pay
- Notifications

Statements

Your latest eBill Statement
Statement (02/15/2017) \$3,267.58 [View](#)

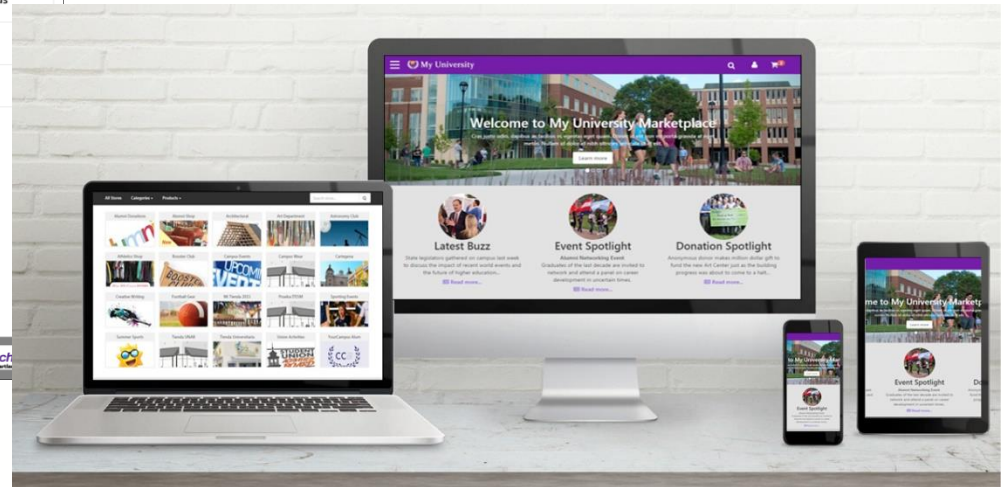
Your latest 1098-T Tax Statement
2016 1098-T Tax Statement [View](#)

Term Balances

Spring Term 2017	\$7,678.23
Fall Term 2016	\$5,063.29
Spring Term 2016	\$3,935.91

© Commerce 7.0 | Bill+Payment 7.0.0
©1997 - 2017 TouchNet Information Systems, Inc. All rights reserved. | TouchNet Privacy Policy

uPay & uStores



In-person: Marketplace POS

“Countertop” Attended payments *At Your Desk*



“Handheld” Attended payments *On The Go*



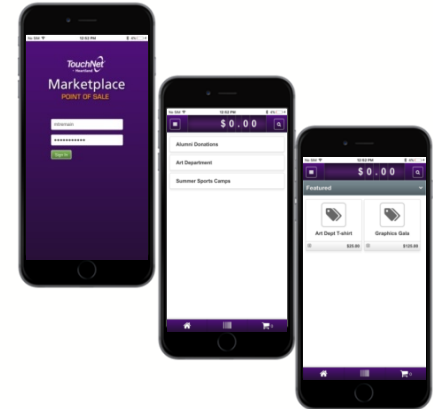
iSMP Companion



iCMP



Blue Bamboo P25i Printer



Other “Cashiering” Solutions

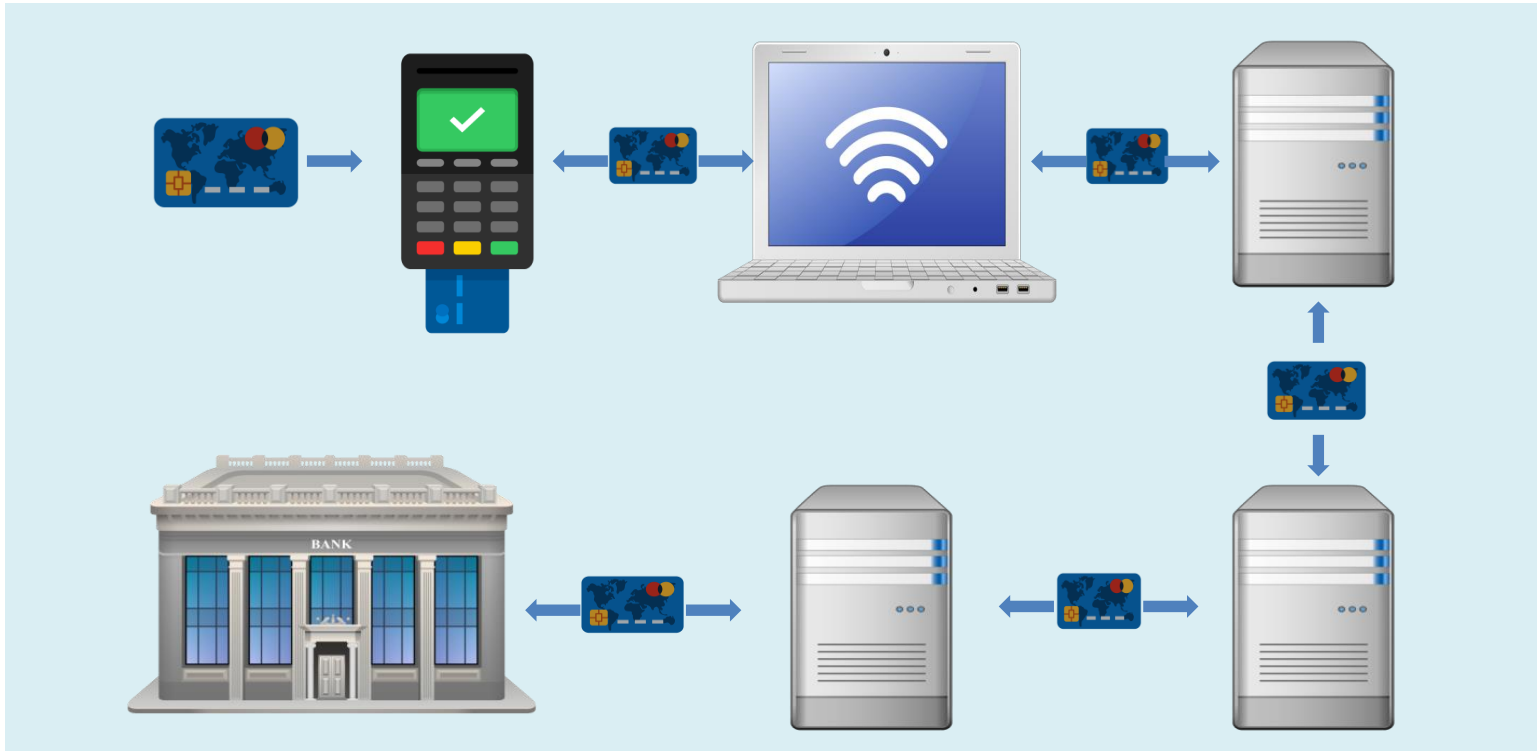
- Student Cashiering



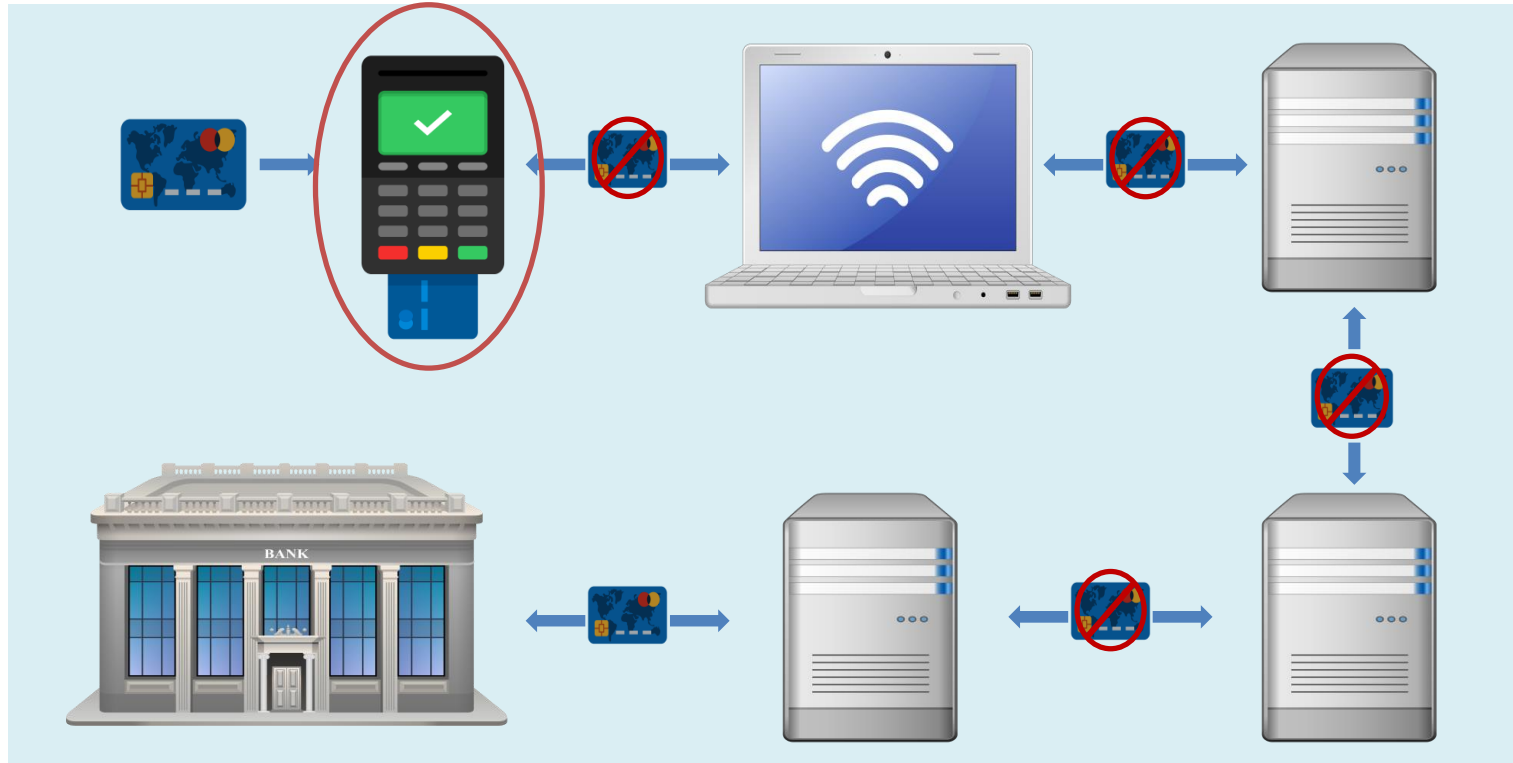
- OneCard Dining | POS



Traditional POS PCI Scope



Validated P2PE Limits “In Scope” to Device Only



The Payment Devices

- EMV Chip Reader
- Secure PIN Pad
- 3-Track MSR
- NFC (Tap & Go)
- Validated P2PE



The U.Commerce Platform

U.Commerce



Reduce Risk and Consolidated PCI Efforts
 Streamline Back-office Operations and Reconciliation

uPay POS with Partners

Controls	U.Commerce Central Dashboard Real-time Alerts RECON 1 RecoverySelect Op Centers Client Community			
Applications	Bill+Payment eStatements (eBills, 1098-Ts) eRefunds Payment Plans SponsorPoint	Cashiering Student Cashiering Departmental Deposits Cashiering Advisor Retail Cashiering	Marketplace uStores Marketplace POS uPay TouchNet Ready Partners	OneCard POS/Dining Access Controls OTC Terminals OneCard Ready Pa
	Payment Center Student Accounts Stored Profiles Parent Pay PCI Payment Gateway Payment Methods Intelligent Routing Transaction Management		OneCard VIP Base Mobile Library Access Check-In/Time ID Verification Declining Balance Events/Recreation ID Management System Web-based Admin Card Station Report Generator	
Integration	Transaction Services RECON 1 PayPath Credit Debit ACH International	ERP Connect Student System Finance/GL Payment Points	Ready Partners TouchNet OneCard Campuswide Vendors	

Commerce Platform



Self Assessment Questionnaires (SAQs)

SAQ	Description	#of Questions	Vulnerability Scan	Penetration Test	SSL/TLS Impact
A	Card-not-present merchants (fully outsourced)	22 (+8)	N	N	N
A-EP	Partially outsourced e-commerce website (direct post)	191 (+52)	Y	Y	Y
B	Card swipe (dial-up), Imprint	41 (0)	N	N	N
B-IP	Card swipe (Internet connected)	82 (-1)	Y	N	Y
C-VT	Web-based virtual terminal	79 (+6)	N	N	Y
C	Payment application connected to Internet	160 (+21)	Y	N	Y
D	All other SAQ-Eligible Merchants	329 (+3)	Y	Y	Y
P2PE	PCI-Listed P2PE Solution	33 (-2)	N	N	N

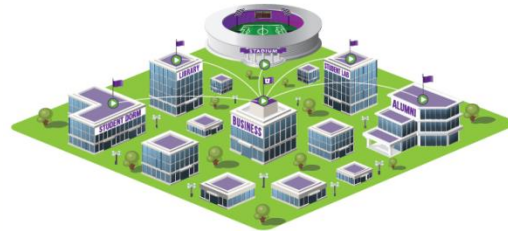
PCI-EZ Strategy: Key #2

1 Platform 

2 Acquirer 

3 ORGANIZE YOUR
MERCHANT STRUCTURE

- PCI Partner / Enforcer
- Dictates SAQs
- Establishes Fee/Fine
- Reconciliation Reports



SAQ SUBMISSION PROCESS



MERCHANT
Submits SAQs
to Acquirer



ACQUIRER
Acquirer reviews and
submits to card brands



CARD BRANDS
Validates merchant
compliance

A gravel road splits into two paths in a forest. The left path is a wide, smooth gravel road that curves slightly to the left. The right path is a narrower, more rustic dirt path with many exposed tree roots and fallen branches. The forest is dense with tall, thin trees and green undergrowth. The text "The PCI" is overlaid in white, bold font in the upper center of the image.

The PCI

Fork in the Road

A photograph of a forest path. On the left, a wide, smooth gravel path curves into the distance. On the right, a narrow, rough dirt path winds through the trees, cluttered with fallen branches and roots. The forest is dense with tall, thin trees and green undergrowth.

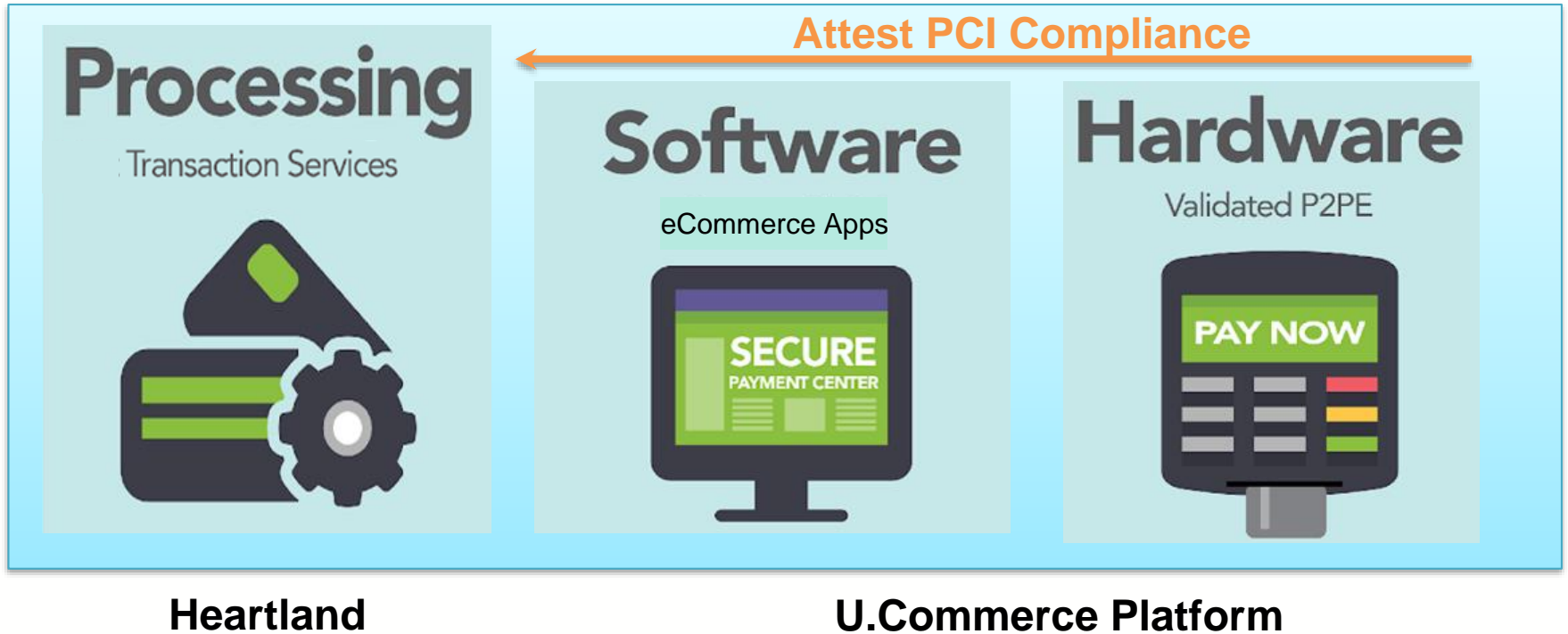
**The
Heartland
Path**

PCI-EZ

**The
Other
Path**

Not as EZ

“Affiliated Acquirer”



PCI-EZ Program











- Integrated QSA Services (ControlScan)
- PCI Expert Assistant (toll-free number)
- Smart SAQs
- Device Exemption Program
- Sample Agreements & FAQ's
- Merchant Training
- Quarterly Vulnerability Scans
- Breach Insurance



The
Heartland
Path

PCI-EZ

What TouchNet Products Do I Have?

 <input type="radio"/> TouchNet Bill+Payment or Bill+Payment Client Please select this method if you leverage TouchNet's Bill+Payment or Bill+Payment Client solution to take integrated student account payments.	 <input type="radio"/> TouchNet PayPath Please select this method if you use TouchNet's PayPath module alongside Bill+Payment to take tuition payments with a service fee.
 <input type="radio"/> TouchNet Cashiering Select this method if you use TouchNet's Cashiering Business Office or Campus Merchant edition to take in-person student account payments campus wide.	 <input type="radio"/> TouchNet Marketplace Select this method if you use Marketplace uStores and/or uPay sites to create, manage, and operate online storefronts and secure payment pages.
 <input type="radio"/> TouchNet Marketplace POS Select his method if you use the ToucNet point of sales integration to take in-person payments through your uStore and/or uPay storefronts.	 <input type="radio"/> TouchNet Ready Partners: TPG Web Service Select this method if you use TouchNet's partner integration to take secure payments through your TouchNet Payment Center(Payment Gateway). If you are using one of the TouchNet Ready Partners listed below please select this option. Active Network, Alliance Software Corporation, Audience View...
 <input type="radio"/> TouchNet Ready Partners: T - Link Select this method if you use TouchNet's partner integration to take secure payments through your connected Marketplace environment.	 <input type="radio"/> TouchNet POS Client (EMV Client) Select this method if you leverage TouchNet's POS Client (EMV Client) integration to you student account system to take point of sale payments through CREN.
 <input type="radio"/> TouchNet Payment Center (Payment Gateway) Select this method if, in addition to using another TouchNet product, you log directly into your customer owned Payment Center (Payment Gateway) and take "Single Auth" pavments.	 <input type="radio"/> Heartland Secure Select this method if you are using one of the following as the ONLY entry mode for cardholder data. Attn: If you are not electronically storing data outside of the Heartland Secure solution, please answer No to the storage question presented on the next screen.

The Turbo Tax Approach to PCI



Introduction Company Environment Qualification Questionnaire Confirmation

Does your business electronically store credit card information?

Do not keep credit card information in electronic files unless necessary.

Electronically storing credit card information means that you are storing the information in a digital format.

Electronic storage only applies to credit card information. Paper copy materials does not count as electronic storage.

YES
 NO

touchnet[®]
A Global Payments Company

Introduction Company Environment Qualification Questionnaire Confirmation

Eligibility

To be eligible to take the reduced Self Assessment Questionnaire A (SAQ A), you must agree to the listed bullet points. If you cannot agree to the eligibility statements, then you must either select a different processing method, OR indicate that you don't agree to the statements in which case you will be directed to complete the full SAQ D-Merchant.

Based on your answers, you qualify to complete a shortened version of the SAQ (SAQ A). Please confirm the following statements:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions.
- All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers.
- Your company has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored.
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all of this data.
- Your company has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant, and
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Additionally, for e-commerce channels:

- The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

Do you agree with all of the above statements?

YES
 NO

Reference: Eligibility

touchnet[®]
A Global Payments Company

Introduction Company Environment Qualification Questionnaire Confirmation

0/22 questions answered 30%

All media is physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

TRUE
 FALSE
 NOT APPLICABLE

For these purposes, "media" refers to all paper and electronic media containing cardholder data.

Reference: SAQ A 9.5

Auto Advance

Step-By-Step Interview Style for SAQ-A

Introduction ✓

Company ✓

Environment ✓

Qualification ✓

Questionnaire >

Confirmation >

59%

1/13 questions answered

Unnecessary default accounts are removed or disabled before installing a system on the network.



- TRUE
- FALSE
- N/A

Reference: SAQ A 2.1b

- 7/13 Questions
- 59% to Completion
- Reference: SAQ A.2.1b

PCI-EZ Portal Resources

touchnet®

A Global Payments Company

[Profile](#) [Home](#) [Support](#) [Sign Out](#)

My Portal **Resources**

PCI Policy Builder

The following templates can be modified to reflect your business environment and help you comply with the PCI DSS information security policy requirements. [Tell me more.](#)

- [SAQ A Security Policy Template](#)
- [SAQ A-EP Security Policy Template](#)
- [SAQ B Security Policy Template](#)
- [SAQ B-IP Security Policy Template](#)
- [SAQ C Security Policy Template](#)
- [SAQ C-VT Security Policy Template](#)
- [SAQ D Security Policy Template](#)
- [SAQ P2PE-HW Security Policy Template](#)

PCI Frequent Questions

- [PCI Compliance](#)
- [PCI Myths](#)
- [PCI Scanning](#)

PCI Links

- [Official PCI Security Standards Council Site](#)
- [Full PCI Data Security Standard](#)
- [PCI Compliance Term Glossary](#)
- [PCI SSC Merchant Microsite](#)
- [Anatomy of a Small Business Data Breach \[VIDEO\]](#)
- [PCI Payment Protection Resources for Small Merchants](#)
- [VISA Security Sense for small business](#)
- [PCI Council: What to do if you have a Data Breach](#)
- [Skimming: A Resource Guide from the PCI Security Standards Council](#)
- [Visa's Global Registry of Service Providers](#)

Breach Protection

The Breach Protection Program is a new and unique indemnification program acquired to reduce monetary exposure in the event of a data compromise.

[More Information](#)

Smart Solutions

Managed Network Firewall



Our Network Firewall ensures that your card data environment is protected against outside threat. We help configure the firewall based on the needs of your business, handle the ongoing firewall updates and patches and ensure that it remains compliant with the PCI DSS.

[Learn More](#)

Security Awareness Training

Learn to protect your business right at the front line where customer interaction takes place.

- [Employee Training](#)
- [Manager Training](#)

[Terms of Use](#) | [Privacy Policy](#)
© 2018 ControlScan. All rights reserved.

PCI Policy Builder

The screenshot shows the touchnet PCI Policy Builder interface. At the top left is the touchnet logo with the tagline 'A Global Payments Company'. Below the logo is a navigation bar with 'My Portal' and 'Resources'. The main heading is 'PCI Policy Builder'. A callout box states: 'These templates are provided for your documentation. The templates are available with the various SAQ types.' Below this, a list of templates is shown: SAQ A Security Policy Template, SAQ A-EP Security Policy Template, SAQ B Security Policy Template, SAQ B-IP Security Policy Template, SAQ C Security Policy Template, SAQ C-VT Security Policy Template, SAQ D Security Policy Template, and SAQ P2PE-HW Security Policy Template. At the bottom, there is a 'PCI Frequent Questions' section with links for PCI Compliance, PCI Myths, and PCI Scanning.

PCI Policy Builder

The following templates can be modified to reflect your business environment and help you comply with the PCI DSS information security policy requirements. [Tell me more.](#)

- SAQ A Security Policy Template
- SAQ A-EP Security Policy Template
- SAQ B Security Policy Template
- SAQ B-IP Security Policy Template
- SAQ C Security Policy Template
- SAQ C-VT Security Policy Template
- SAQ D Security Policy Template
- SAQ P2PE-HW Security Policy Template

Security Awareness Training

ControlScan

End-User Security Awareness (EUSA) Certificate Program - Foundation Course

End-User Security Awareness (EUSA) Certificate Program
Foundation Course

ANSI
ANSI ACCREDITED PROGRAM
CERTIFICATE ISSUER

© 2006 – 2015 SCIPP International, Inc. All Rights Reserved

Menu Notes

- 1. Module 1
 - 1.1. Introduction
 - 1.2. Overview
 - 1.3. Pre-Assessment
 - 1.4. What is Information Security?
 - 1.5. Information Security Awareness
 - 1.6. Business Requirements
 - 1.7. Key Elements of Information Security
 - 1.8. Best Business Practices 1-10
 - 1.9. (1) Policies/Compliance - Your Responsibilities
 - 1.10. (2) Internet - Avoid Communication Hazards
 - 1.11. (3) Access Controls - Never Share with Others
 - 1.12. (4) Human Resources - It's All About the People
 - 1.13. (5) Asset Management - Protect Your Valuables

Search...

◀ ▶ 🔍 ↻ NEXT ▶



PCI Compliance Validation Exemption Program(s)



(Visa Client Name) _____ (Visa Business ID) _____ (Date) _____
 (Merchant Company Name) _____ (Merchant Country) _____

Instructions for Submission

Visa acquirer must complete all applicable sections and submit application to local Visa Payment System Risk team. *Note: Incomplete applications or those submitted for merchants not meeting criteria will not be accepted.*

Merchant Level: (check one) Level 1 Level 2 Level 3 Level 4

Visa Client Confirms:

- Merchant validated PCI DSS compliance. YES NO
(Validation is not a condition for approval.)
- Merchant confirmed that sensitive authentication data (i.e., full contents of magnetic stripe, CVV2 or PIN data) is not stored on any system subsequent to transaction authorization.
- Merchant has not been involved in breach of cardholder data.
- At least 75% of merchant's transactions originate through one of the following secure acceptance channels:
 - Enabled chip-reading terminals¹ (U.S. merchants must use dual interface terminals)
 - Validated² Point-to-Point Encryption (P2PE) Solution

P2PE Solution Name:

¹ Chip-enabled terminals must have current, valid EMV approval and pass Acquirer Device Validation Toolkit (ADVT) / Contactless Evaluation Toolkit (CET) / Visa PayWave Test Tool (VPTT) testing requirements, as applicable.
² Point-to-Point Encryption solution must be included on PCI SSC's list of validated solutions or validated by a PCI SSC Qualified Security Assessor P2PE Company.

(Signature of Visa Acquirer Officer) _____ (Date) _____
 (Acquirer Officer Name) _____ (Title) _____

Discover Information Security & Compliance (DISC) Program Merchant EMV PCI Validation Waiver Application



Merchant EMV Waiver Eligibility

This waiver application applies to Merchants who have a minimum of 75% of their transactions processed through Chip Terminals enabled to accept Chip Card Transactions (including, without limitation, Discover D-PAS transactions). Merchants must have previously validated PCI DSS Compliance or provided their PCI DSS certified approach/ remediation plan to Discover to be considered eligible for this waiver.

Instructions for Submission:

Discover Merchant must complete each of the below sections and submit this waiver application to the Discover Data Security team at DISCCCompliance@discover.com

Section 1: Merchant Information

Merchant Name: _____
 Doing Business As: _____
 Merchant Level (select one): Level 1 Level 2 Level 4

Section 2: Merchant Attestation

I, the Merchant named above, attest to the following:

- Merchant is not storing Sensitive Authentication Data (i.e., full contents of magnetic stripe, CVV2, CID or PIN data) on any system subsequent to transaction authorization
- At least 75% of Merchant's transactions originated from Chip Card Terminals¹ enabled to accept Chip Card Transactions (including, without limitation, Discover D-PAS transactions)
¹ Chip Card Terminals must have current, valid EMV approval and Discover D-PAS Certification.
- Merchant has documented and annually tests a Data Security Breach incident response program in accordance with the Payment Card Industry Data Security Standard requirements
- Merchant has not been involved in a Data Security Breach in the past 12 months

Section 3: Data Security Contact

Merchant must complete the information below designating a primary contact for any Data Security matters.

Name	Title
Phone#	
Email	

Section 4: Authorized Approval

This form must be signed by an individual with signatory authority at the Merchant.

Signature	Title	Date
Print Name	E-mail	Phone#

American Express® Annual Security Technology Enhancement Program (STEP) Attestation

The American Express Data Security Operating Policy requires merchants, among several things, to provide documentation validating compliance with the PCI Data Security Standard (PCI DSS). Merchants who have adopted certain security enhancements may instead submit this STEP Attestation.

Step 1: Annual Self-Examination

- Merchants conduct an annual self-examination of their equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted to validate that they have adopted one or more of the following security enhancements and meet the remaining attestation criteria. This annual self-examination is to be performed by a person designated from within your company. Your chief executive officer, chief financial officer, chief information security officer, or authorized signer for the organization must sign the Attestation form. Compliance and validation are completed at your expense. By submitting this attestation, you represent and warrant to American Express that you are authorized to disclose the information contained therein and are providing the attestation to American Express without violating any other party's rights. American Express may verify the results of your STEP Attestation validation process by up to, and including, engaging, at American Express's expense, a Qualified Security Assessor (QSA) of our choice to complete an on-site assessment of your company's security environment. The Attestation expires one year from the signature date. You must reassess your security environment and resubmit this STEP Attestation of Compliance annually.

Step 2: Attestation

- We comply with all requirements of the current PCI Data Security Standard (PCI DSS), as available at www.pcisecuritystandards.org
- A minimum of 75% of our total American Express Card Transactions are made:
 - Through EMV compliant terminals OR
 - Using a Point-To-Point Encryption (P2PE) solution included on the PCI SSC list of validated solutions OR
 - Using a Point-To-Point Encryption (P2PE) solution that has been validated by a PCI SSC Qualified Security Assessor
- We have not been involved in a data incident which compromised American Express Card Members' information within the twelve (12) months prior to the signature date of this Annual STEP Attestation.
- The undersigned hereby attest that all of the statements in this STEP Attestation are true and accurate.

Merchant Name
 American Express Merchant Number (3D digit SEP)
 Merchant Phone Number
 Merchant Data Security Contact Email Address
 Name of person completing Attestation
 Title of person completing Attestation
 Signature Date (YYYY-MM-DD)
 Signature of authorized signer

Step 3: Report

- Option 1:** Save completed form as a PDF. Visit <https://login.truwave.com> to access the Trustwave secure portal and upload your completed STEP Attestation.
- Option 2:** Print completed form and send via fax to Trustwave at 1-312-276-4018 (if you are in an international market add the appropriate international calling sequence. International charges may apply).
- Option 3:** Save completed form as a PDF. Send via email to AmericanExpressCompliance@trustwave.com. If you need assistance submitting the form contact Trustwave at AmericanExpressCompliance@trustwave.com.

Definitions

- PCI DSS** - The Payment Card Industry Data Security Standard, which is available at <https://www.pcisecuritystandards.org>.
- Point-to-point encryption (P2PE)** solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.
- EMV compliant terminal** - A Chip-Enabled Device having a valid and current EMVCo (www.emvco.com) approval/certification and capable of processing ACQ compliant Chip Card Transactions.
- Qualified Security Assessor, or QSA**, means an entity that has been qualified by the Payment Card Industry Security Standards Council, LLC to render adherence to the PCI DSS.

Security Technology Enhancement Program Attestation, April 2017



Validated P2PE With Heartland



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



SAQ Exemption With Heartland



SOFTWARE
TouchNet Payment Center



HARDWARE
Validated P2PE



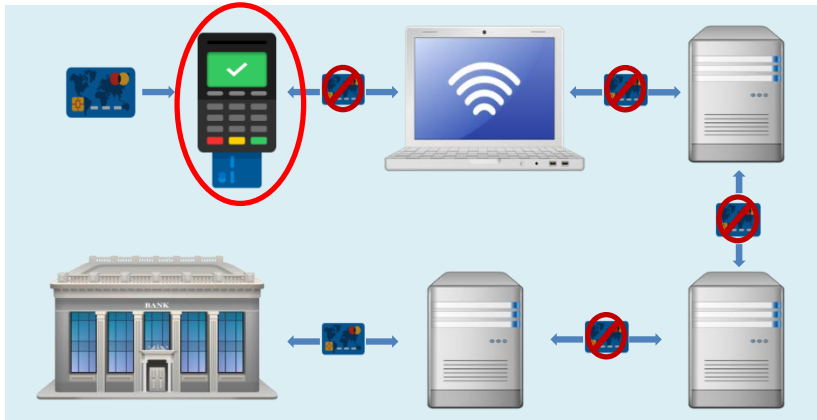
PROCESSING
TouchNet Transaction Services

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



Benefits for All, Affiliated (or not)

- All Merchants (All Acquirers)
 - Validated Point-to-Point Encryption
 - U.Commerce Platform + Partners




	U.Commerce Central			
Controls	Dashboard Real-time Alerts RECON 1 RecoverySelect Op Centers Client Community			
Applications	Bill+Payment •Statements (eBills, 1098-T) •Refunds Payment Plans SponsorPoint	Cashiering Student Cashiering Departmental Deposits Cashiering Advisor Retail Cashiering	Marketplace uStores Marketplace POS uPay TouchNet Ready Partners	OneCard POS/Dining Access Controls OTC Terminals OneCard Ready Partners
	Payment Center Student Accounts Stored Profiles Parent Pay Scheduled Payments Consent Manager Automated Alerts PCI Payment Gateway Payment Methods Intelligent Routing Transaction Management		OneCard VIP Base Mobile Library Access Checkin/Time Events/Recreation ID Verification Declining Balance ID Management System Web-based Admin Card Station Report Generator	
Integration	Transaction Services RECON 1 PayPath Credit Debit ACH International	ERP Connect Student System Finance/GL Payment Points	Ready Partners TouchNet OneCard Campuswide Vendors	

A gravel path winds through a forest of tall, thin trees. The path is wide and well-maintained, curving to the right. The surrounding forest is dense with green foliage and many tree trunks. The text 'The Heartland Path' is overlaid in white on the left side of the path, and 'PCI-EZ' is overlaid in white at the bottom left of the path.

**The
Heartland
Path**

PCI-EZ

A dirt path winds through a forest of tall, thin trees. The path is narrow and appears to be a natural trail, with many fallen branches and roots on the ground. The surrounding forest is dense with green foliage and many tree trunks. The text 'The Other Path' is overlaid in white on the right side of the path.

**The
Other
Path**

PCI-EZ

Not as EZ

PCI-EZ Recap

- Integrated QSA Services (ControlScan)
- Smart SAQs
- Device Exemption Program
- Sample Agreements & FAQ's
- Merchant Training
- PCI Expert Assistant
- Quarterly Vulnerability Scans
- Breach Insurance



The
Heartland
Path

PCI-EZ

PCI-EZ Strategy: Key #3

1 Platform



2 Acquirer



3 ORGANIZE YOUR
MERCHANT STRUCTURE



SAQ SUBMISSION PROCESS



MERCHANT

Submits SAQs
to Acquirer



ACQUIRER

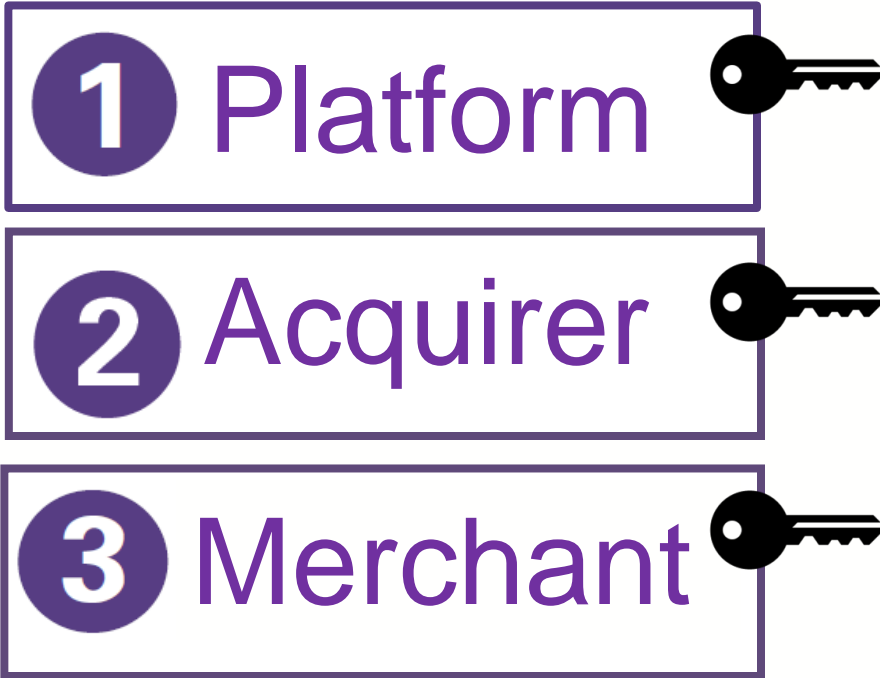
Acquirer reviews and
submits to card brands



CARD BRANDS

Validates merchant
compliance

PCI-EZ Strategy: Key #3



touchnet[®]
A Global Payments Company

[Home](#) [Live Chat](#) [Email](#) [Phone](#)

Menu

- Compliance Overview
- News 📰
- PCI Resources
- Security Awareness
- General FAQs
- Feedback
- Settings
- Logout

Compliance Overview at a Glance

TouchNet Demo

Merchant ID: 121820171

Overall PCI Compliance Status

Requires questionnaire

Annual Questionnaire

Questionnaire not started as of 2017-12-18

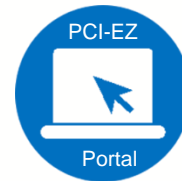
Next Action:

[Click here to start your Questionnaire](#)

[Prioritized Approach Report](#)

Merchant (You) – Executing The Plan

- Build a team
- Set and enforce a policy*
- Provide merchant training*
- Track your devices*
- Picking the right partners
- Organizing your merchant structure**



*

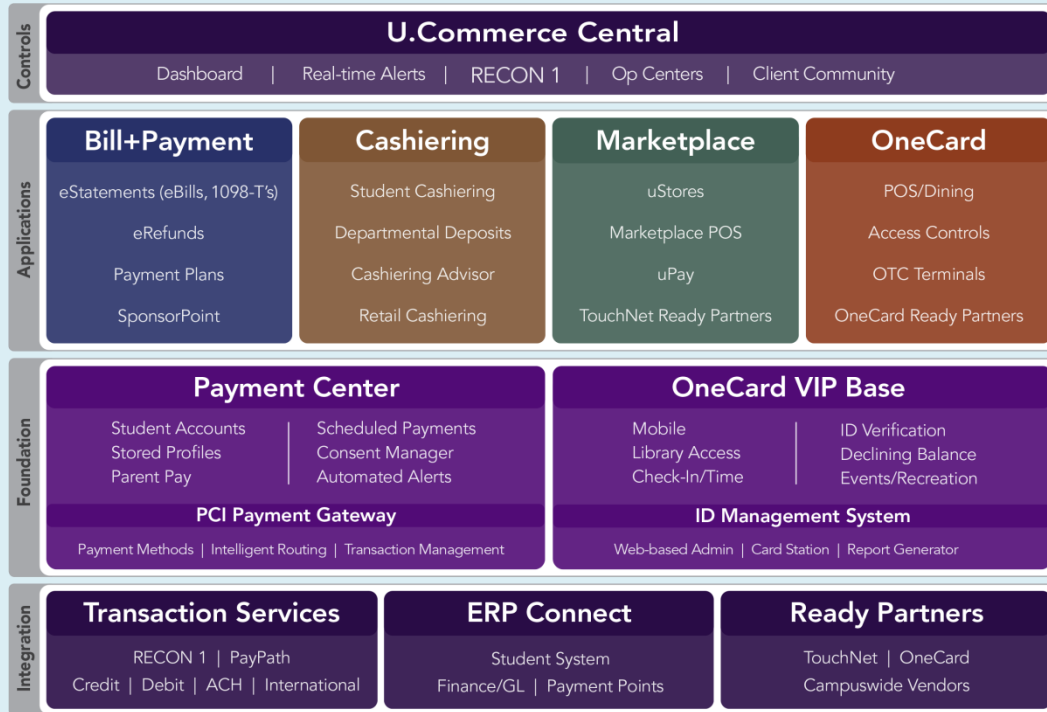


**

The Hackers Don't Sleep



Starts with the Platform



Include Devices

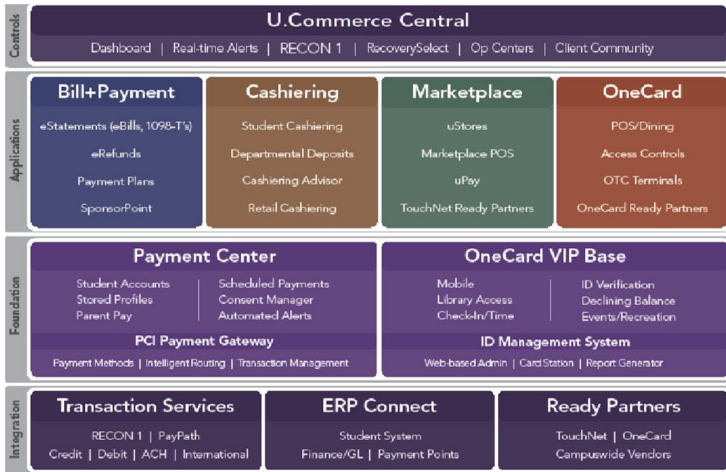
Controls	U.Commerce Central Dashboard Real-time Alerts RECON 1 RecoverySelect Op Centers Client Community			
Applications	Bill-Payment eStatements (eBills, 1098-Ts) eRefunds Payment Plans SponsorPoint	Cashiering Student Cashiering Departmental Deposits Cashiering Advisor Retail Cashiering	Marketplace uStores Marketplace POS uPay TouchNet Ready Partners	OneCard POS/Dining Access Controls OTC Terminals OneCard Ready Pa
	Payment Center Student Accounts Scheduled Payments Stored Profiles Consent Manager Parent Pay Automated Alerts PCI Payment Gateway Payment Methods Intelligent Routing Transaction Management		OneCard VIP Base Mobile ID Verification Library Access Declining Balance Check-In/Time Events/Recreation ID Management System Web-based Admin Card Station Report Generator	
Integration	Transaction Services RECON 1 PayPath Credit Debit ACH International	ERP Connect Student System Finance/GL Payment Points	Ready Partners TouchNet OneCard Campuswide Vendors	

Commerce Platform



Partner/Vendor Strategy

U.Commerce



Reduce Risk and Consolidated PCI Efforts
Streamline Back-office Operations and Reconciliation

QUESTIONS?

touchnet[®]

A Global Payments Company

Thanks!

Dave Swan, Reginal Sale Manager
david.swan@touchnet.com

touchnet[®]

A Global Payments Company