Payment Card Industry (PCI) Data Security Standards

Understanding & Achieving Compliance at Independent Schools

www.diamondmindinc.com

DiamondMind
Payment Solutions for Schools

Trusted Partner to Private Schools

Acting as an Extension of Your Business Office Staff

Dedicated to Private Schools

$2B+ Funds Processed Annually

1500+ Happy Clients

99% Customer Retention

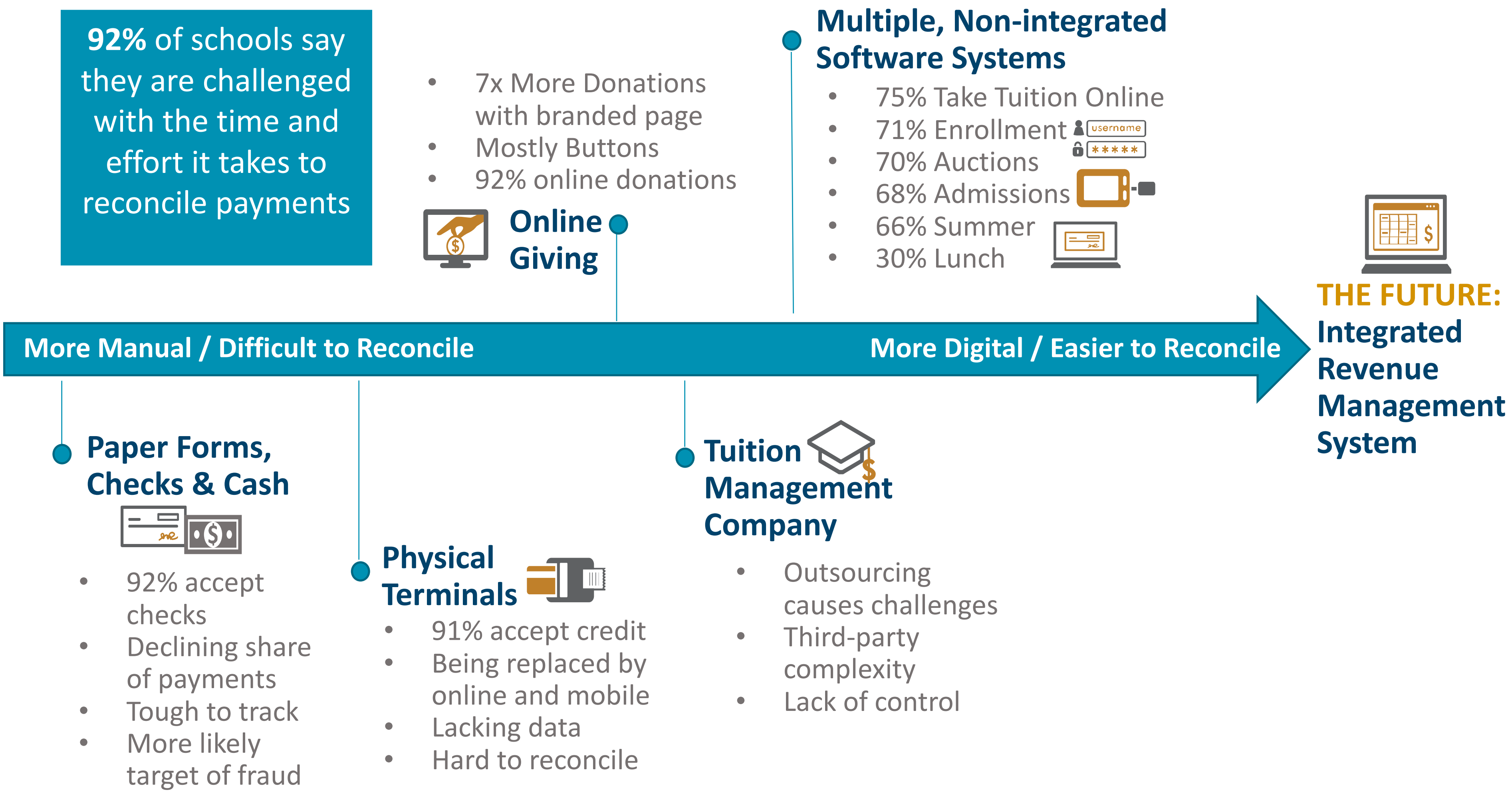
Who we are…

- ✓ Private School Specialists
- ✓ Payment Processing Experts

What we believe in…

- ✓ Simple & Affordable Solutions
- ✓ Transparency
- ✓ Flexibility & Choice

Evolution of Payments at Private Schools



92% of schools say they are challenged with the time and effort it takes to reconcile payments

More Manual / Difficult to Reconcile

More Digital / Easier to Reconcile

Paper Forms, Checks & Cash

- 92% accept checks
- Declining share of payments
- Tough to track
- More likely target of fraud

Physical Terminals

- 91% accept credit
- Being replaced by online and mobile
- Lacking data
- Hard to reconcile

Online Giving

- 7x More Donations with branded page
- Mostly Buttons
- 92% online donations

Tuition Management Company

- Outsourcing causes challenges
- Third-party complexity
- Lack of control

Multiple, Non-integrated Software Systems

- 75% Take Tuition Online
- 71% Enrollment
- 70% Auctions
- 68% Admissions
- 66% Summer
- 30% Lunch

THE FUTURE: Integrated Revenue Management System

Sources: 2016 Digital Payment Trends at Independent Schools Survey, Diamond Mind, MISBO, PAISBOA

The Dramatic Shift to Digital

From Paper Checks to Digital Payments

15% of Payments

Paper Checks

- Payments Deposited in 1 Week
- Slows Down Cash Flow
- Manual Data Entry
- Missing Information
- Difficult Reconciliation
- Most Susceptible to Fraud
- Days before Bounce Notification

77% of Payments

eChecks & Credit Cards

- Daily Deposits
- Accelerates Cash Flow
- Digital Data Entry
- Complete Information
- Easy Reconciliation
- Least Susceptible to Fraud
- Online Insufficient Funds Check

Sources: 2013 Federal Reserve Payment Study; 2016 Diamond Mind Survey

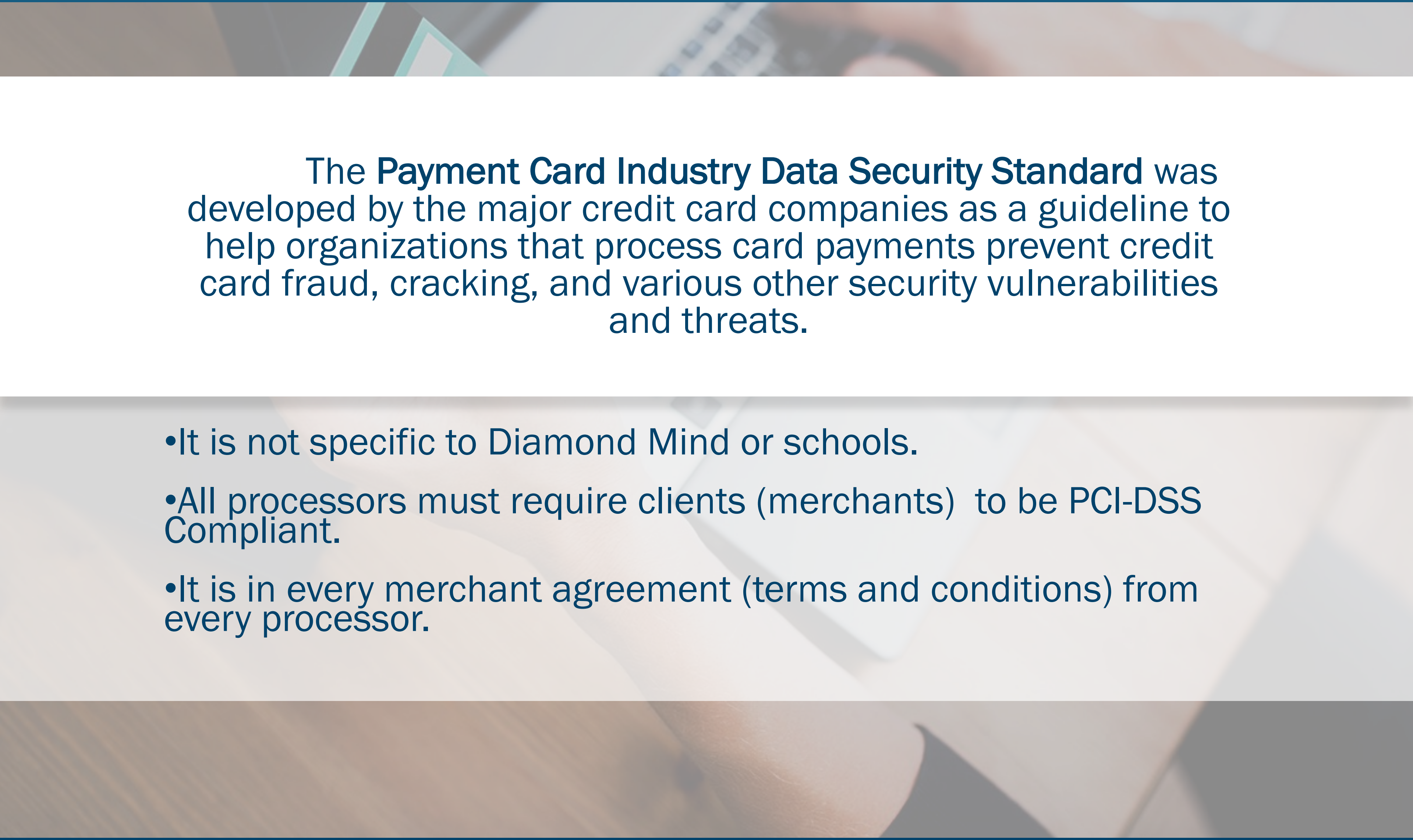
PCI-DSS Learning Objectives

- Provide clear understanding of your Payment Card Industry Data Security Standard Responsibilities

- Share a practical step-by-step plan for achieving Payment Card Industry Data Security Standard Compliance

- Explain the interdependencies between your school, your vendors' PCI-DSS status, and your ability to achieve Payment Card Industry Data Security Standard Compliance

What is the Payment Card Industry Data Security Standard (PCI-DSS)?



The **Payment Card Industry Data Security Standard** was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, cracking, and various other security vulnerabilities and threats.

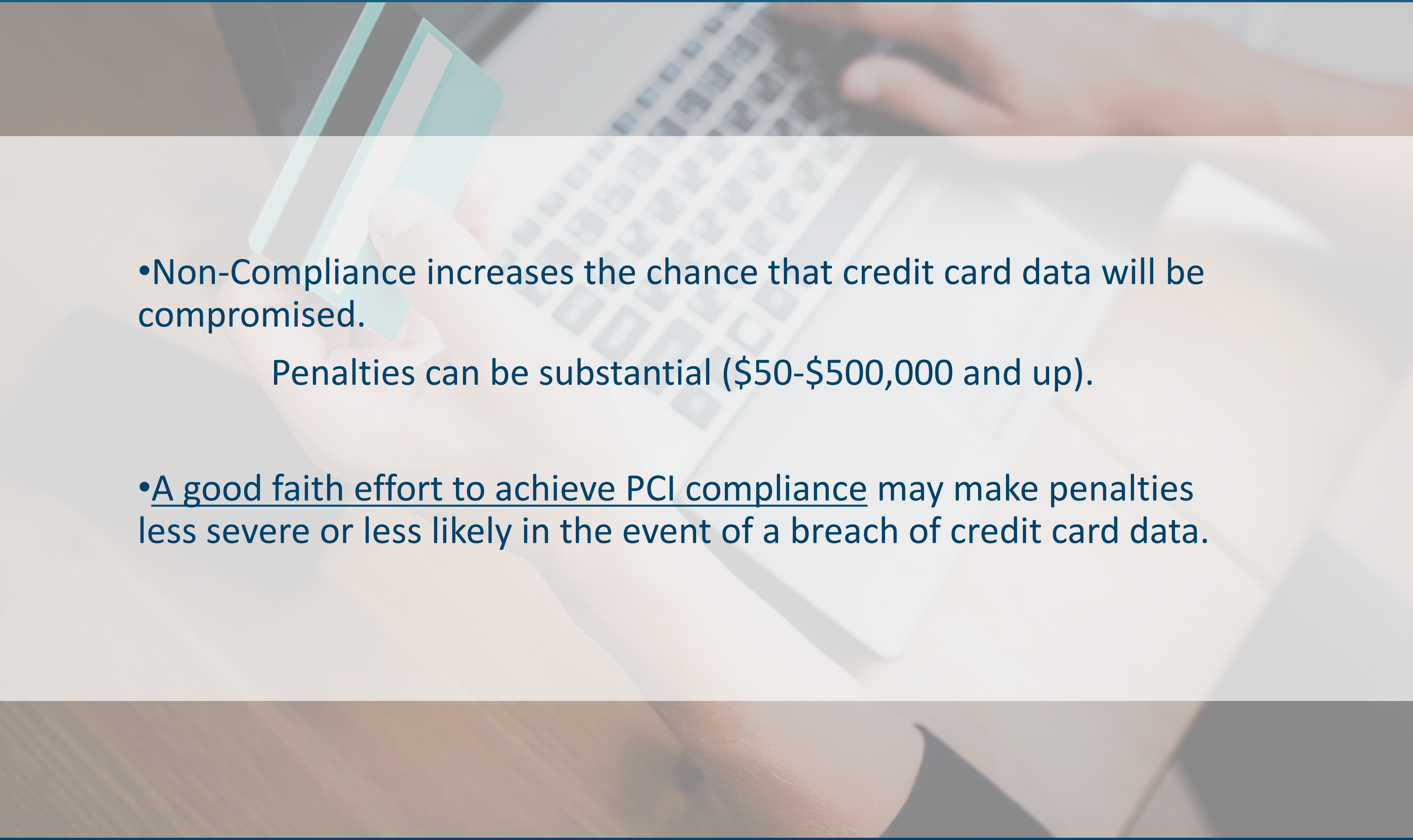
- It is not specific to Diamond Mind or schools.
- All processors must require clients (merchants) to be PCI-DSS Compliant.
- It is in every merchant agreement (terms and conditions) from every processor.

What is PCI-DSS vs. PA-DSS

The **Payment Card Industry Data Security Standard applies to all** entities that process, store or transmit payment card data.

- All such entities must be PCI DSS compliant or risk losing their ability to process credit card payments and being audited and/or fined.
- Payment Application Data Security Standard (PA-DSS) is a subset of requirements that Payment Application Providers that transmit credit card data must adhere in order for you to meet PCI-DSS compliance

Risk and Cost of Non-Compliance

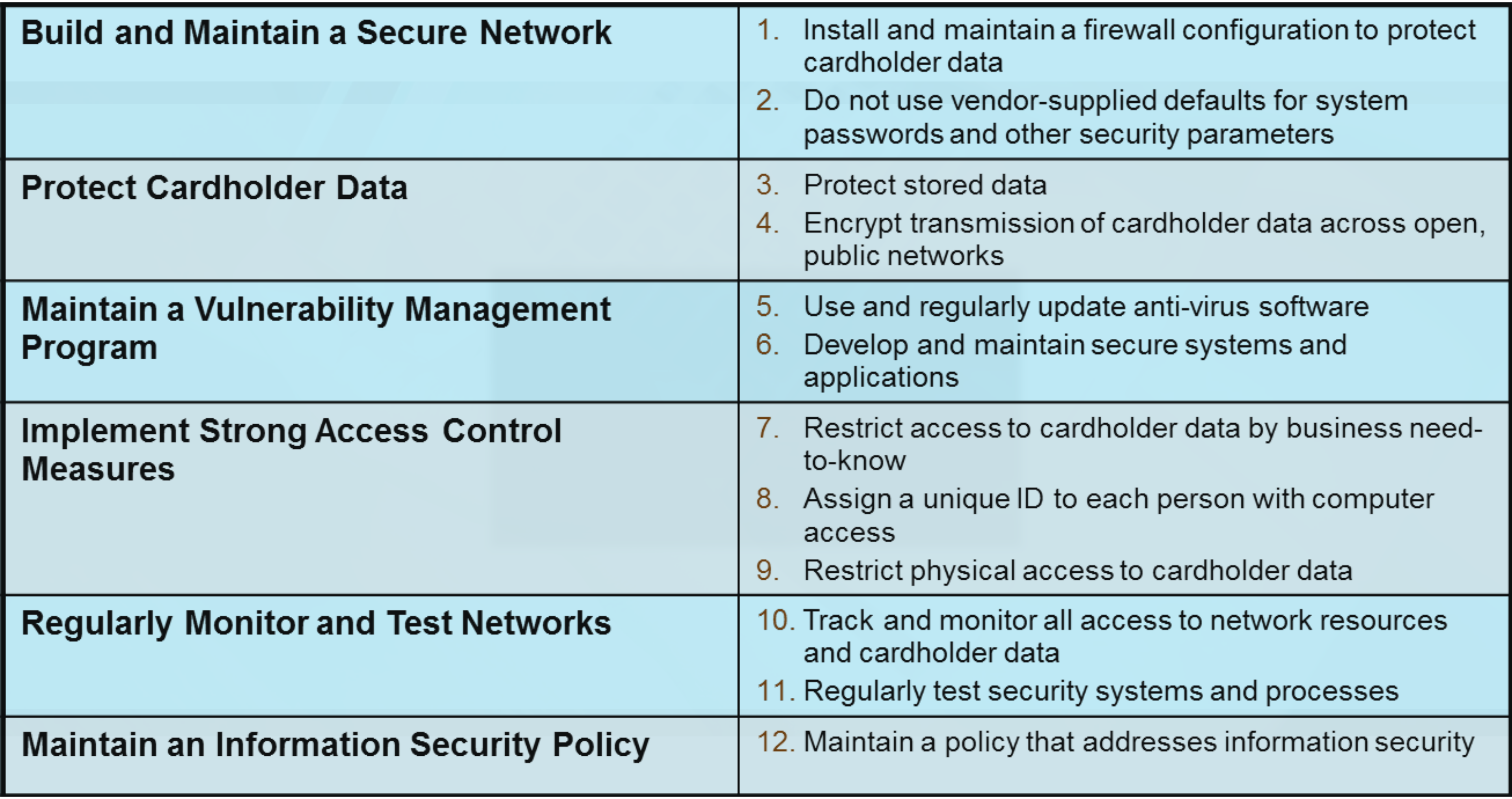


- Non-Compliance increases the chance that credit card data will be compromised.

  Penalties can be substantial ($50-$500,000 and up).

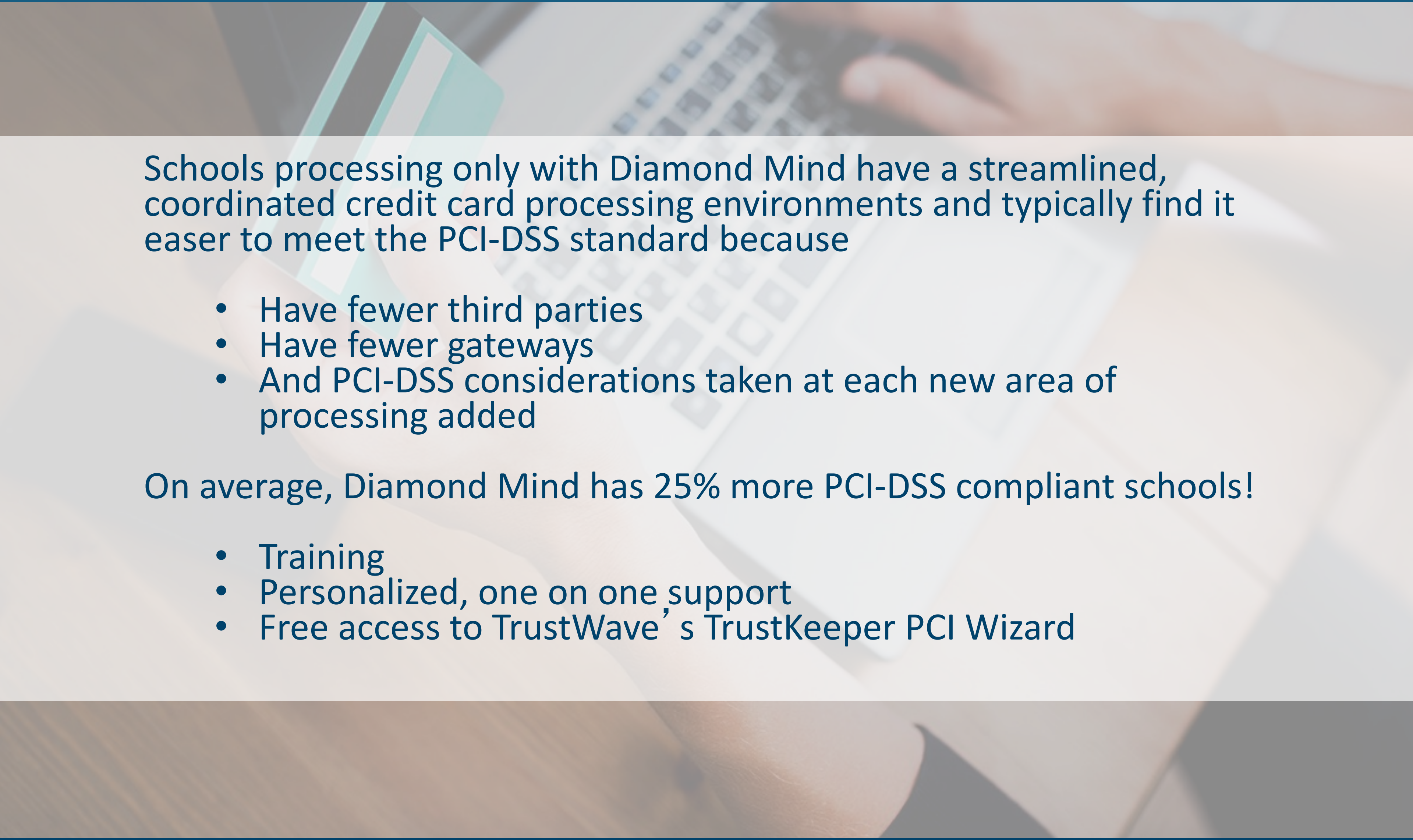
- A good faith effort to achieve PCI compliance may make penalties less severe or less likely in the event of a breach of credit card data.

Requirements Overview



Build and Maintain a Secure Network	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 data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 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

Diamond Mind, Making PCI-DSS Compliance Easier!



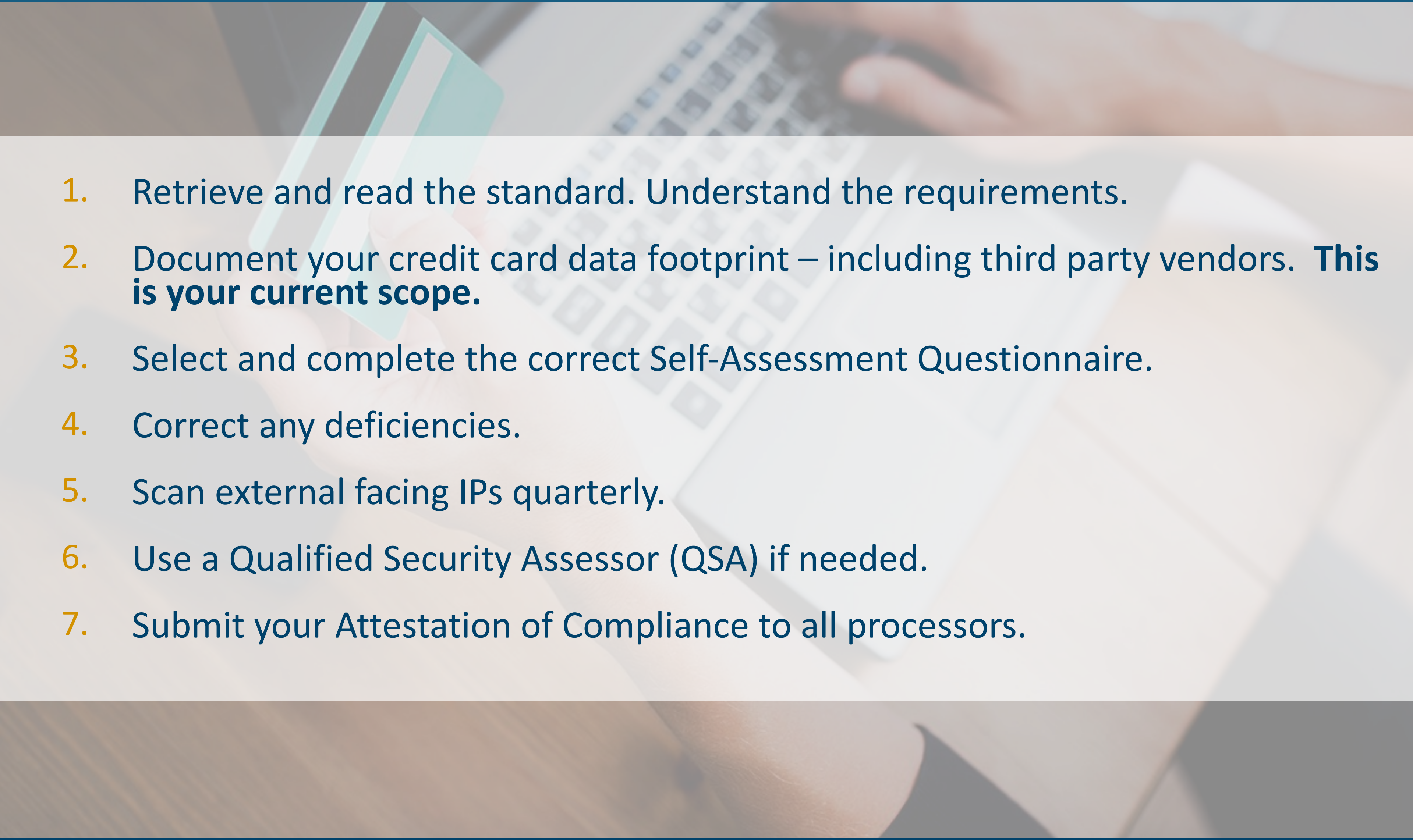
Schools processing only with Diamond Mind have a streamlined, coordinated credit card processing environments and typically find it easer to meet the PCI-DSS standard because

- Have fewer third parties
- Have fewer gateways
- And PCI-DSS considerations taken at each new area of processing added

On average, Diamond Mind has 25% more PCI-DSS compliant schools!

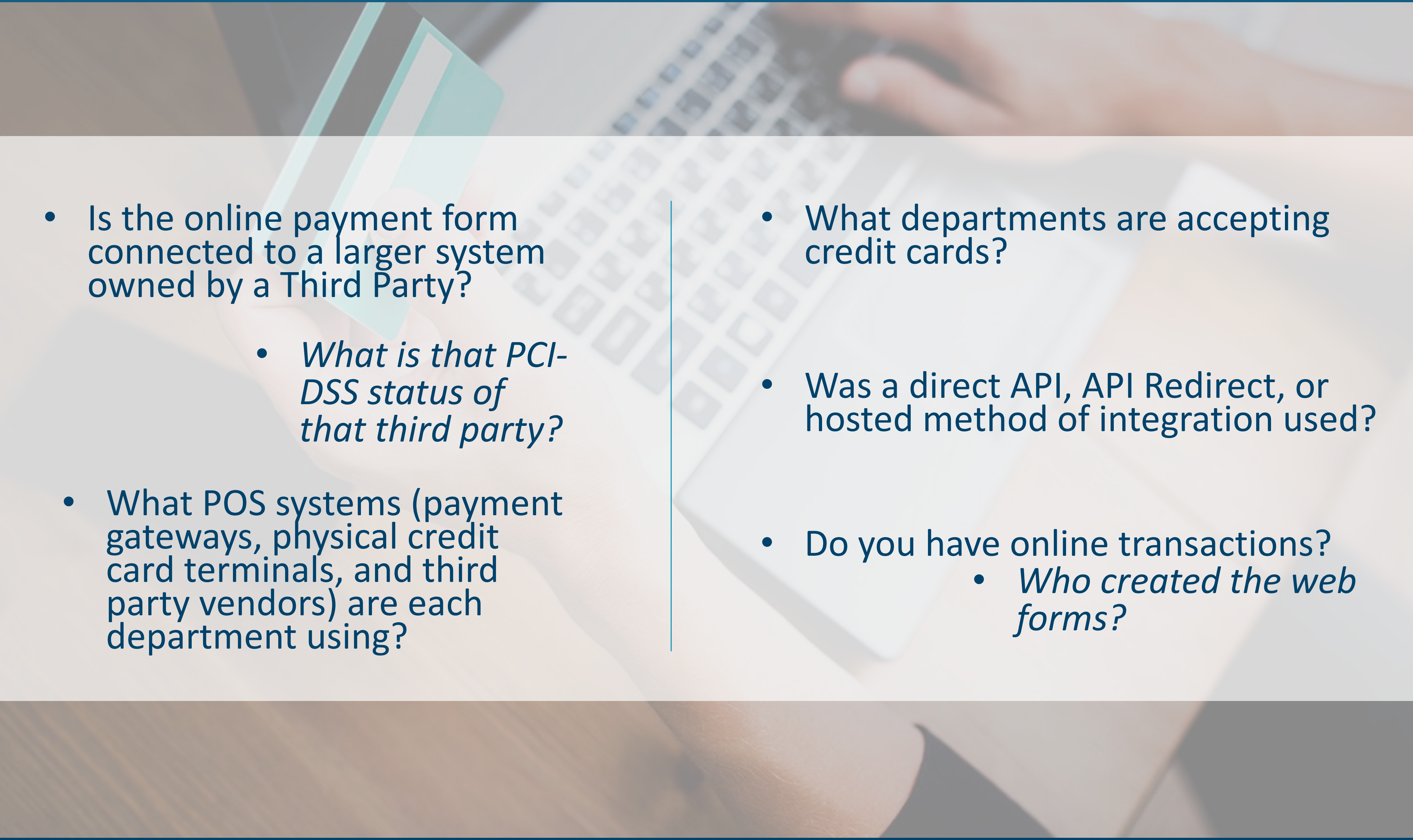
- Training
- Personalized, one on one support
- Free access to TrustWave’s TrustKeeper PCI Wizard

Seven Easy Steps



1. Retrieve and read the standard. Understand the requirements.
2. Document your credit card data footprint – including third party vendors. **This is your current scope.**
3. Select and complete the correct Self-Assessment Questionnaire.
4. Correct any deficiencies.
5. Scan external facing IPs quarterly.
6. Use a Qualified Security Assessor (QSA) if needed.
7. Submit your Attestation of Compliance to all processors.

Determining Your Scope



- Is the online payment form connected to a larger system owned by a Third Party?
  - *What is that PCI-DSS status of that third party?*
- What POS systems (payment gateways, physical credit card terminals, and third party vendors) are each department using?
- What departments are accepting credit cards?
- Was a direct API, API Redirect, or hosted method of integration used?
- Do you have online transactions?
  - *Who created the web forms?*

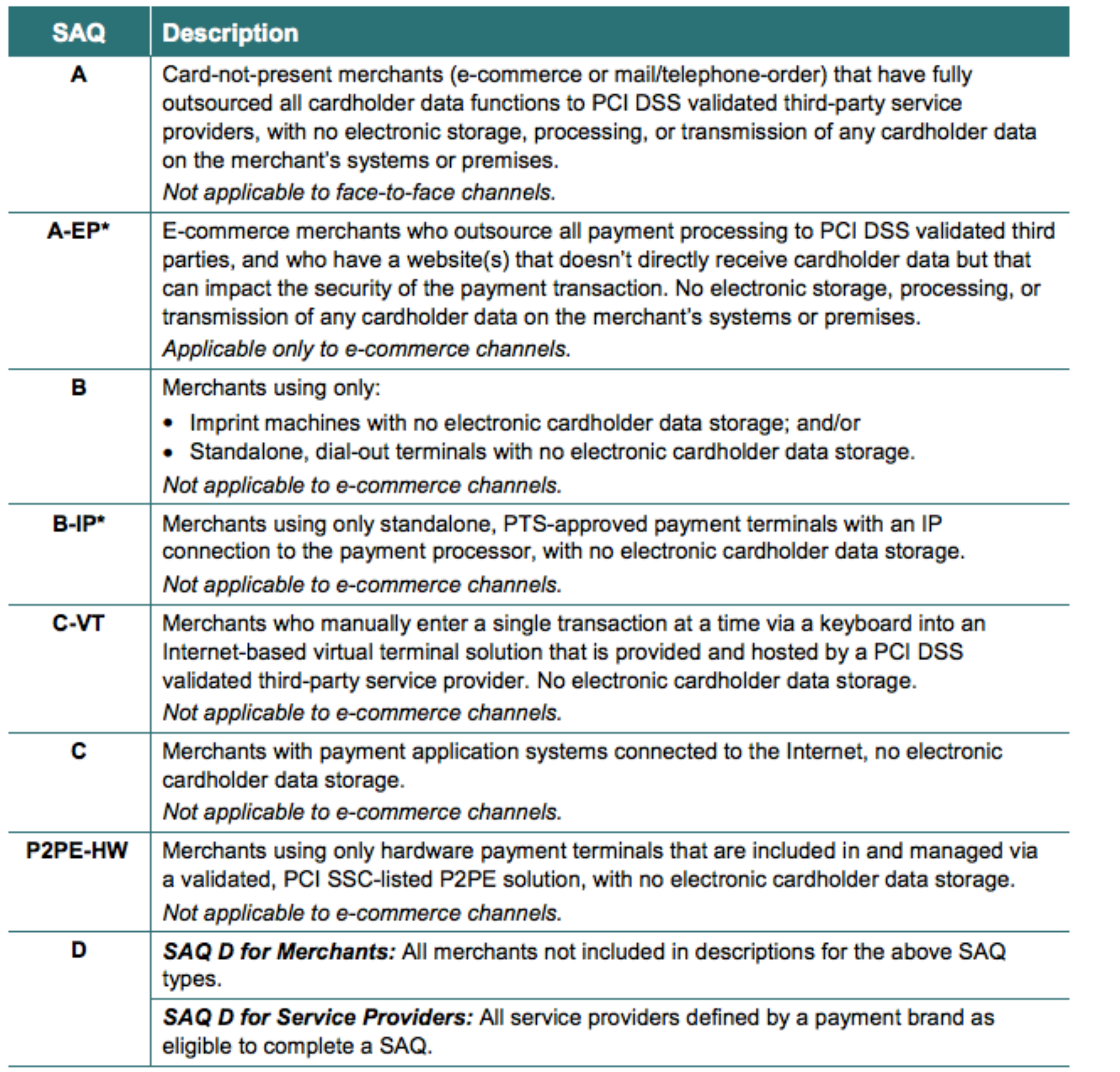
Online Forms and Web Application Providers

If your form providers and web applications (in-house or 3rd party provided) are not PCI or PA-DSS compliant, and credit card data flows through them, then you are not compliant.

DISCOVER NETWORK MasterCard VISA AMERICAN EXPRESS

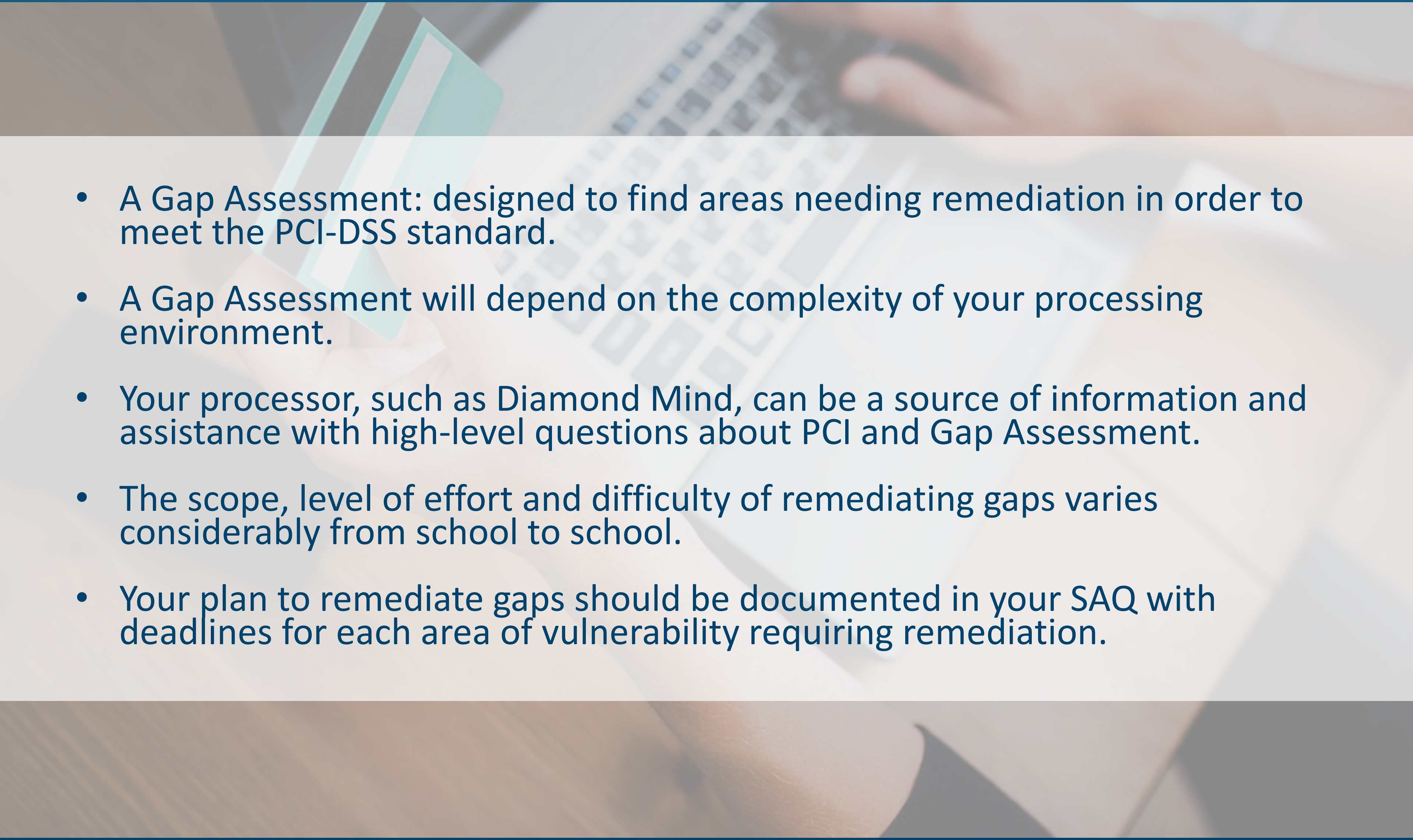
You must still ensure your own PCI-DSS Compliance and document it in (at a minimum) a SAQ Questionnaire annually.

Choosing the Right SAQ



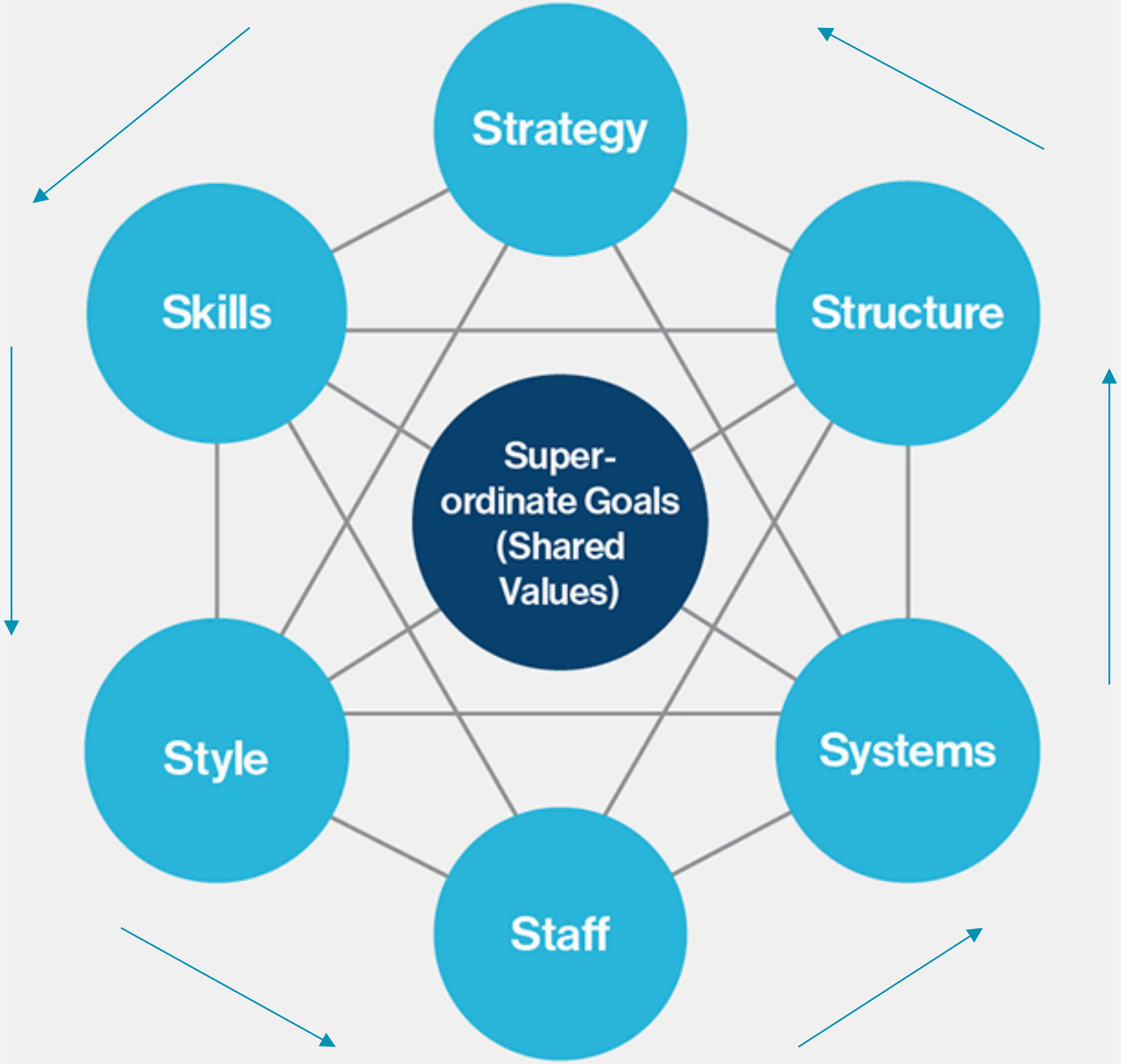
SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Conduct a GAP Assessment
Compare your Environment to the PCI Standard

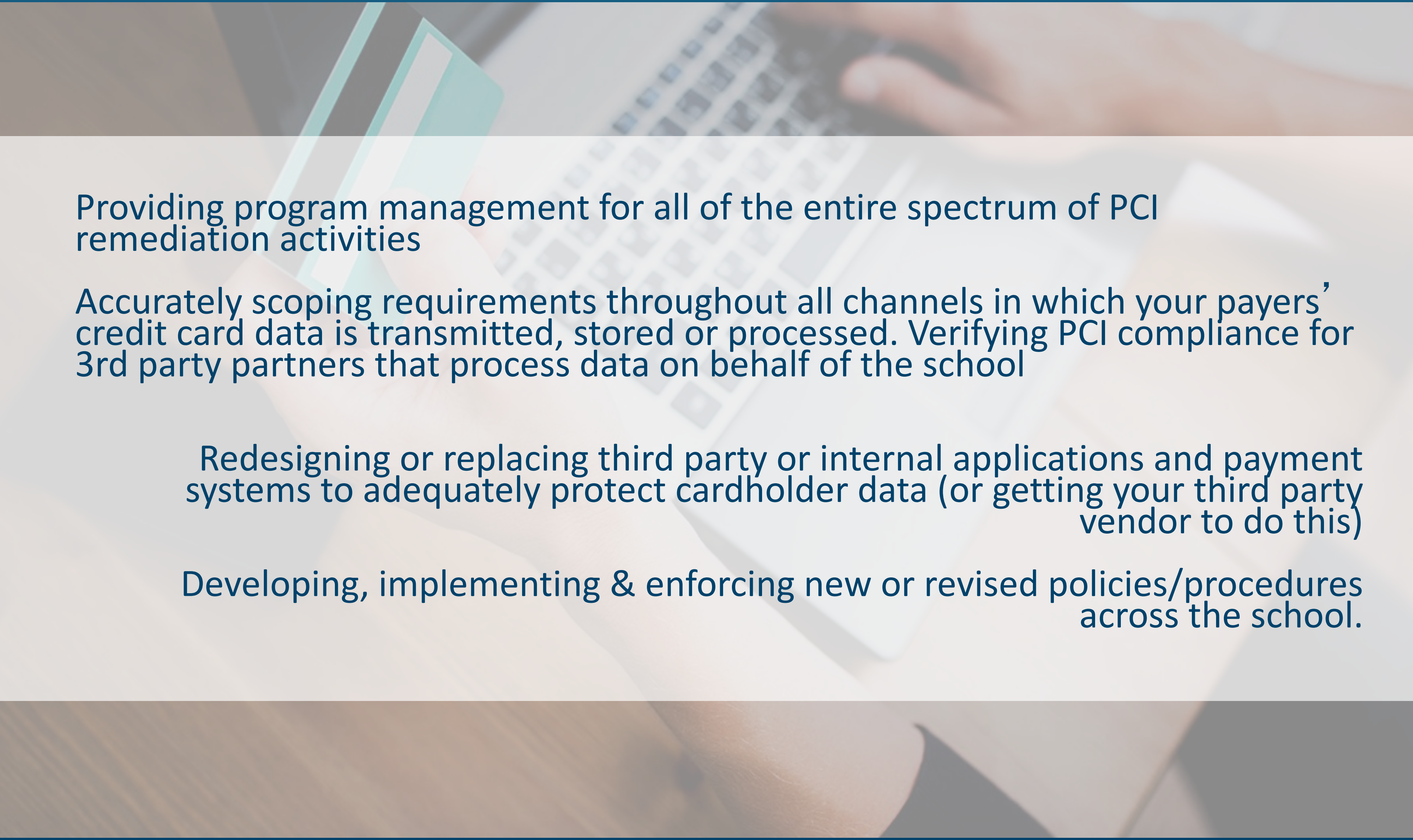


- A Gap Assessment: designed to find areas needing remediation in order to meet the PCI-DSS standard.
- A Gap Assessment will depend on the complexity of your processing environment.
- Your processor, such as Diamond Mind, can be a source of information and assistance with high-level questions about PCI and Gap Assessment.
- The scope, level of effort and difficulty of remediating gaps varies considerably from school to school.
- Your plan to remediate gaps should be documented in your SAQ with deadlines for each area of vulnerability requiring remediation.

GAP Assessment



Challenges to the GAP Assessment



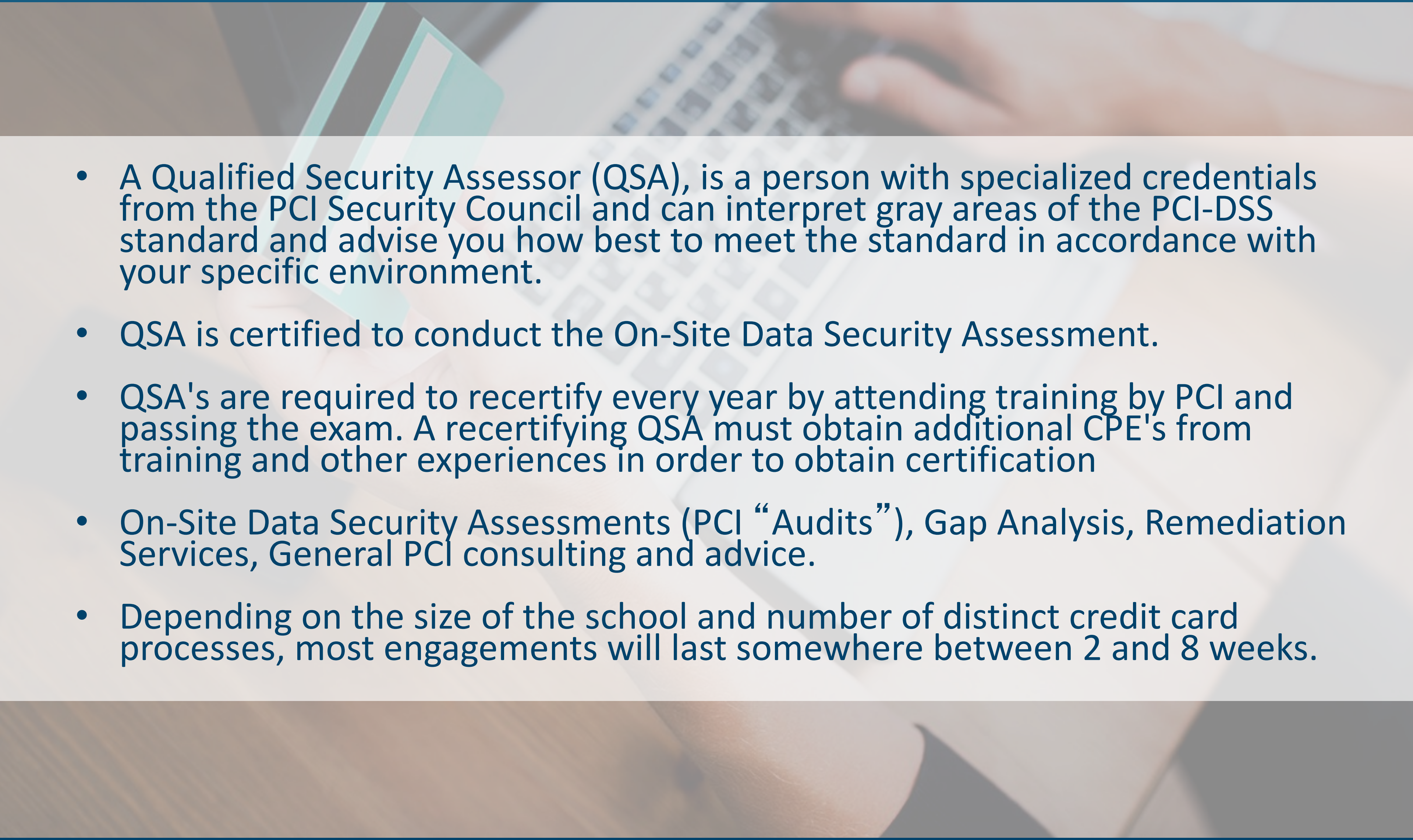
Providing program management for all of the entire spectrum of PCI remediation activities

Accurately scoping requirements throughout all channels in which your payers' credit card data is transmitted, stored or processed. Verifying PCI compliance for 3rd party partners that process data on behalf of the school

Redesigning or replacing third party or internal applications and payment systems to adequately protect cardholder data (or getting your third party vendor to do this)

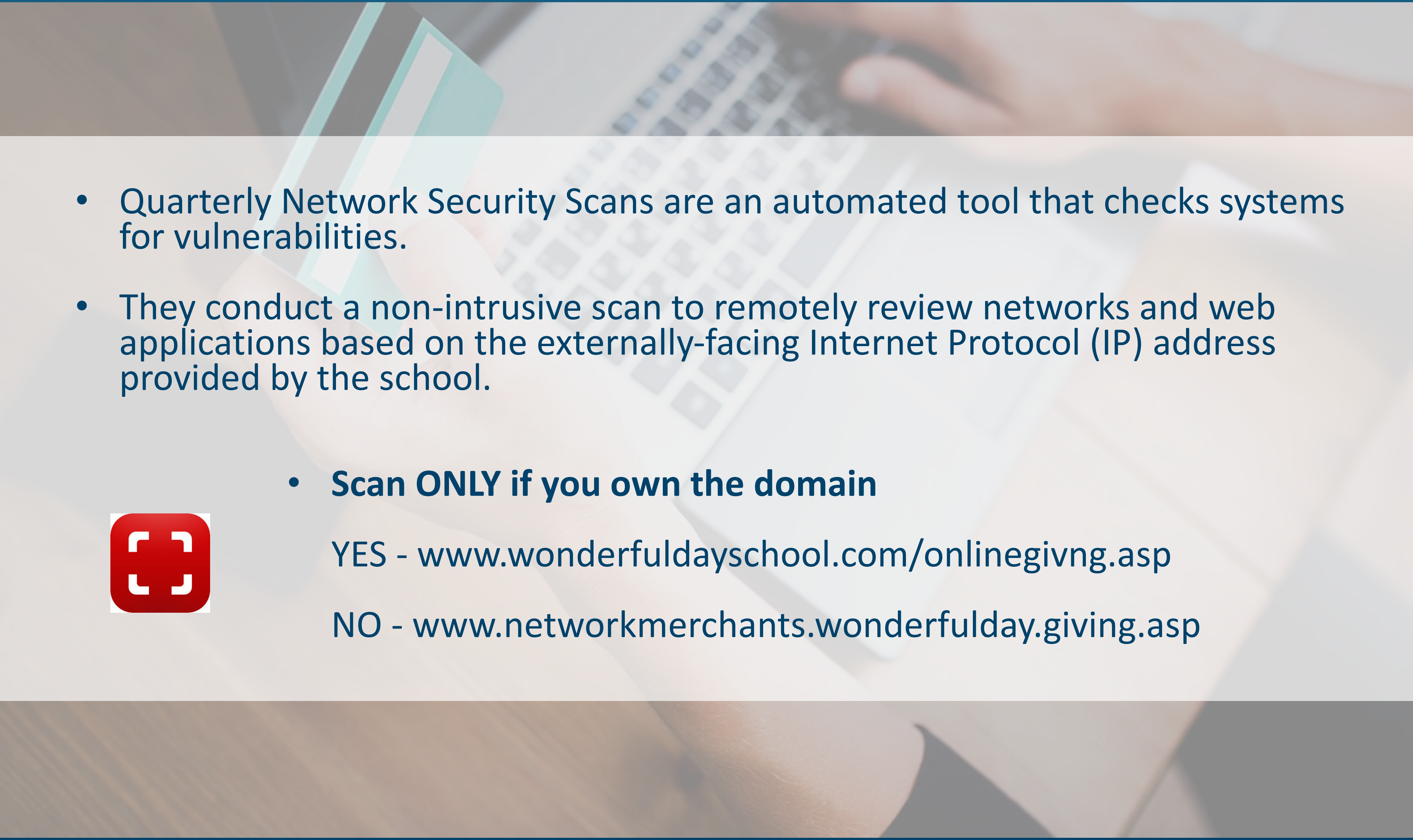
Developing, implementing & enforcing new or revised policies/procedures across the school.

Engaging A QSA



- A Qualified Security Assessor (QSA), is a person with specialized credentials from the PCI Security Council and can interpret gray areas of the PCI-DSS standard and advise you how best to meet the standard in accordance with your specific environment.
- QSA is certified to conduct the On-Site Data Security Assessment.
- QSA's are required to recertify every year by attending training by PCI and passing the exam. A recertifying QSA must obtain additional CPE's from training and other experiences in order to obtain certification
- On-Site Data Security Assessments (PCI “Audits”), Gap Analysis, Remediation Services, General PCI consulting and advice.
- Depending on the size of the school and number of distinct credit card processes, most engagements will last somewhere between 2 and 8 weeks.

Quarterly Scan Requirements



- Quarterly Network Security Scans are an automated tool that checks systems for vulnerabilities.
- They conduct a non-intrusive scan to remotely review networks and web applications based on the externally-facing Internet Protocol (IP) address provided by the school.

- **Scan ONLY if you own the domain**

YES - www.wonderfuldayschool.com/onlinegivng.asp

NO - www.networkmerchants.wonderfulday.giving.asp

Most Common PCI-DSS Vulnerabilities

1. STORAGE
2. ACCESS
3. PASSWORDS
4. POOR CODING
5. OUTDATED PATCHES/SOFTWARE
6. MONITORING
7. LACK OF SEGMENTATION

Almost Done!

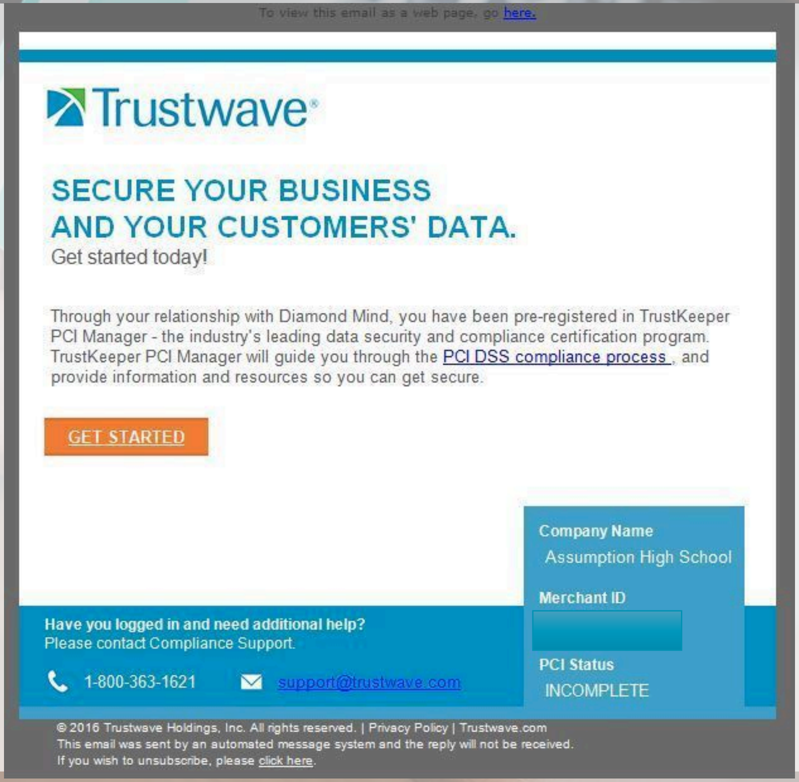
- Manage PCI-DSS Compliance and Repeat SAQ annually
- If you add new areas of credit card processing reevaluate if you’ ll need to complete a different SAQ

- Complete the SAQ: Send to your credit card processing companies
- If you’ re not meeting requirements in some areas, create a plan with dates to address these areas

Diamond Mind and TrustWave

- TrustWave is a Threat, Vulnerability, and Compliance Management Partner
- TrustWave's TrustKeeper cloud and managed security services portal is offered at no cost to all Diamond Mind schools.
- Includes Penetration Testing, Compliance Management, and vulnerability scanning and more for free!
- 24 Hour, 7 days per week, 365 days per year support

Getting Started with Diamond Mind



To view this email as a web page, go here.

Trustwave®

SECURE YOUR BUSINESS AND YOUR CUSTOMERS' DATA.

Get started today!

Through your relationship with Diamond Mind, you have been pre-registered in TrustKeeper PCI Manager - the industry's leading data security and compliance certification program. TrustKeeper PCI Manager will guide you through the PCI DSS compliance process , and provide information and resources so you can get secure.

Company Name
Assumption High School

Merchant ID
[redacted]

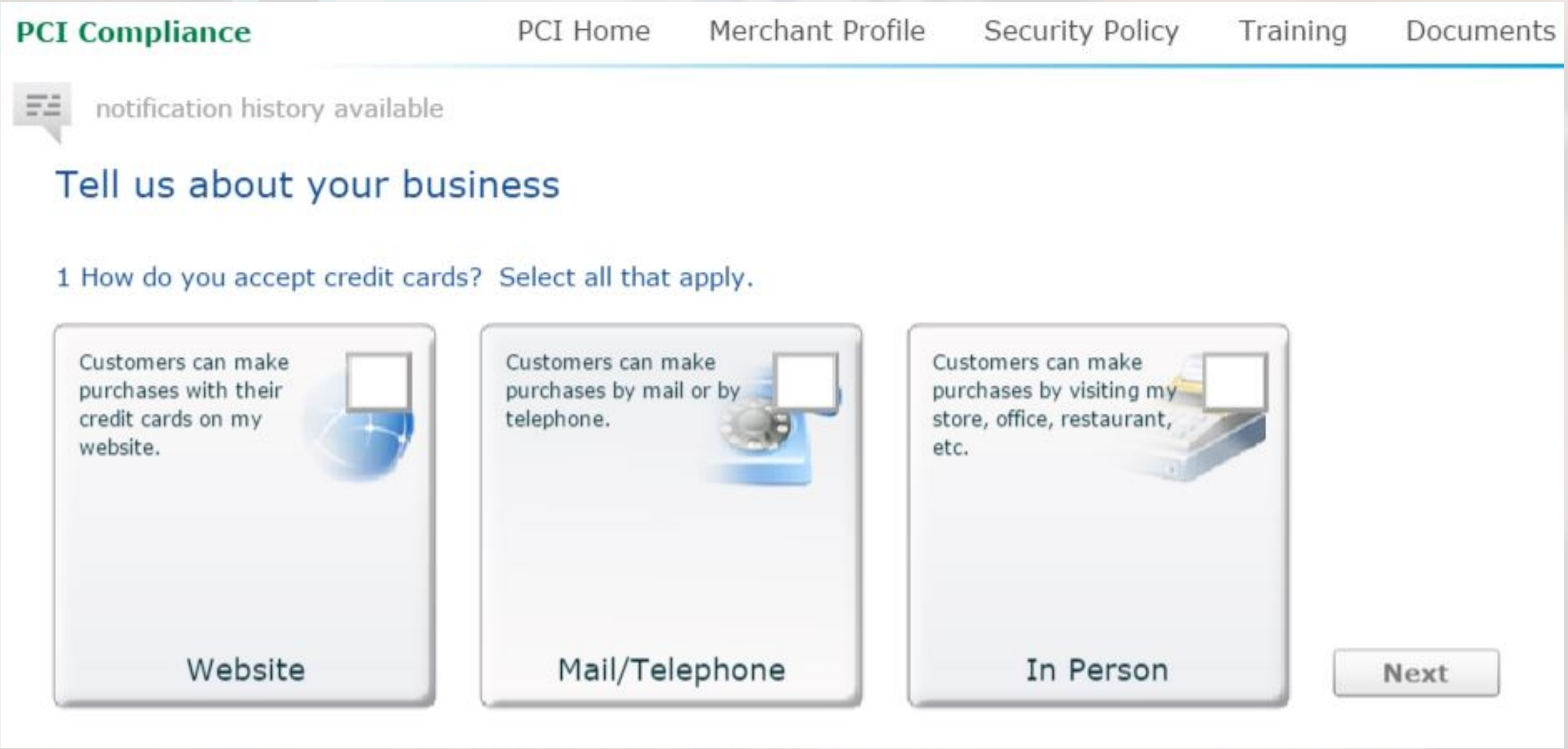
PCI Status
INCOMPLETE

Have you logged in and need additional help?
Please contact Compliance Support.

☎ 1-800-363-1621 ✉ support@trustwave.com

© 2016 Trustwave Holdings, Inc. All rights reserved. | Privacy Policy | Trustwave.com
This email was sent by an automated message system and the reply will not be received.
If you wish to unsubscribe, please click here.

TrustWave-Your Business Environment



Tell us about your business

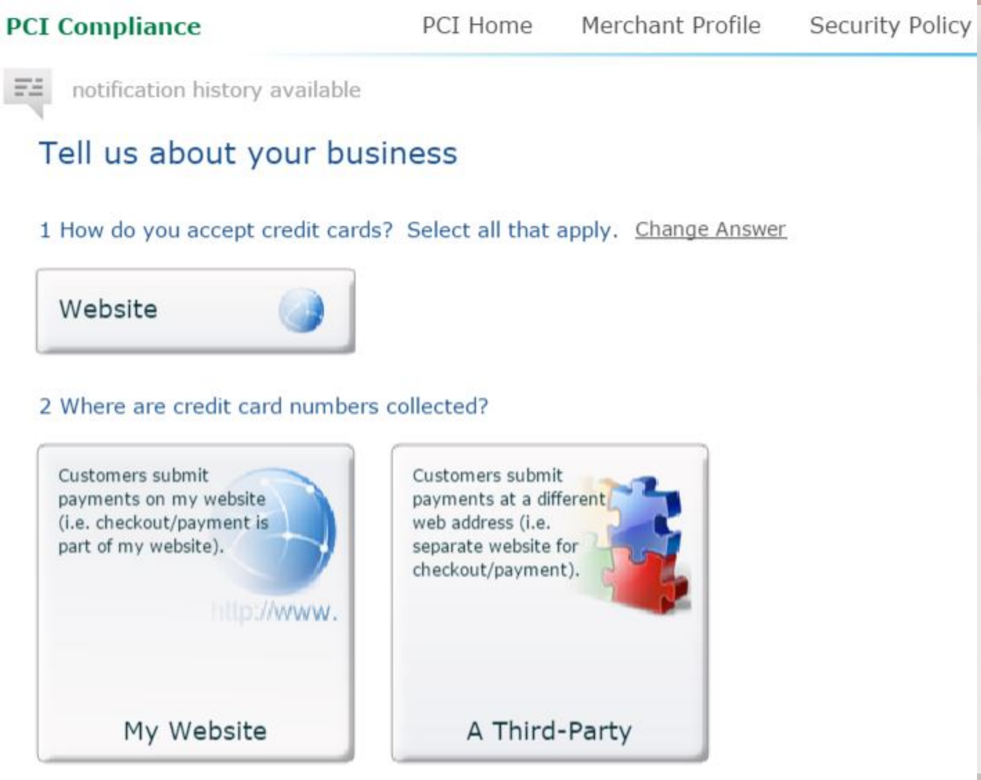
1 How do you accept credit cards? Select all that apply.

□ Customers can make purchases with their credit cards on my website.
Website

□ Customers can make purchases by mail or by telephone.
Mail/Telephone

□ Customers can make purchases by visiting my store, office, restaurant, etc.
In Person

TrustWave-About Your Business



Tell us about your business

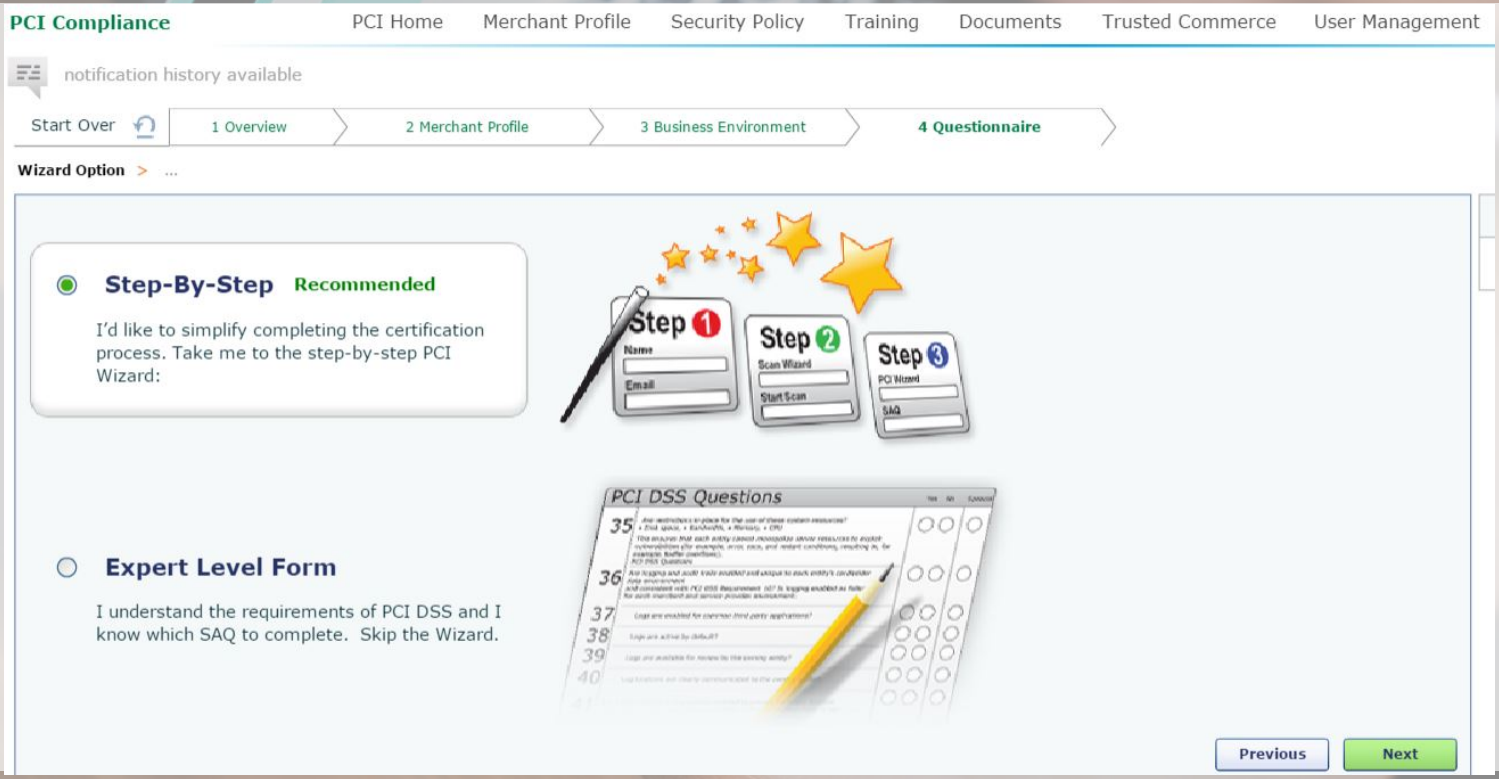
1 How do you accept credit cards? Select all that apply. Change Answer

2 Where are credit card numbers collected?

Customers submit payments on my website (i.e. checkout/payment is part of my website).

Customers submit payments at a different web address (i.e. separate website for checkout/payment).

TrustWave-Getting Started is Easy!



PCI Compliance

notification history available

Wizard Option > ...

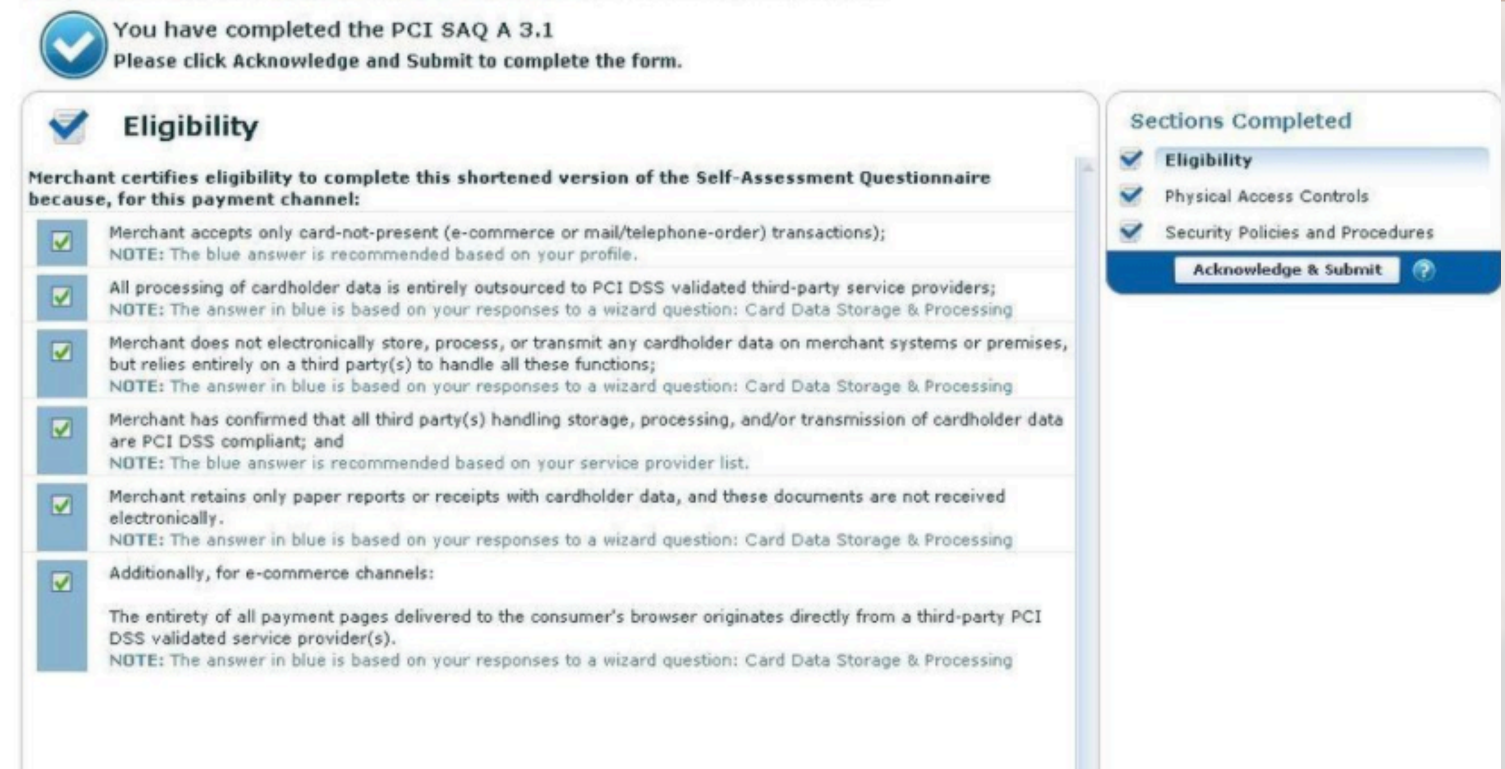
● **Step-By-Step** Recommended

I'd like to simplify completing the certification process. Take me to the step-by-step PCI Wizard:

○ **Expert Level Form**

I understand the requirements of PCI DSS and I know which SAQ to complete. Skip the Wizard.

Submitting Through TrustWave



You have completed the PCI SAQ A 3.1

Please click Acknowledge and Submit to complete the form.

✓ Eligibility

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

☑ Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
NOTE: The blue answer is recommended based on your profile.

☑ All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
NOTE: The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing

☑ Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
NOTE: The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing

☑ Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
NOTE: The blue answer is recommended based on your service provider list.

☑ Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.
NOTE: The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing

☑ 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).
NOTE: The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing

Sections Completed
✓ Eligibility
✓ Physical Access Controls
✓ Security Policies and Procedures
Acknowledge & Submit

True Cost of Manual Processes & Payment Silos

Visible and hidden costs of inefficiencies in the process

30 – 50
Wasted Hours
Per Month

Manual Processes & Lack of Control or Visibility

- Time to manually process paper checks and forms
- Hours coordinating with multiple vendors and processors
- Time to reconcile with other depts. (e.g. Development) all using different software and/or processors

15% - 40%
Higher Cost

Multiple Vendors & Technologies

- Spending more than necessary on processing costs
- Increased costs from multiple vendor's monthly and annual fees
- Confusing or hidden fees from payment processors

30%+
Lost Revenue
Opportunity

Lost Revenue Opportunity

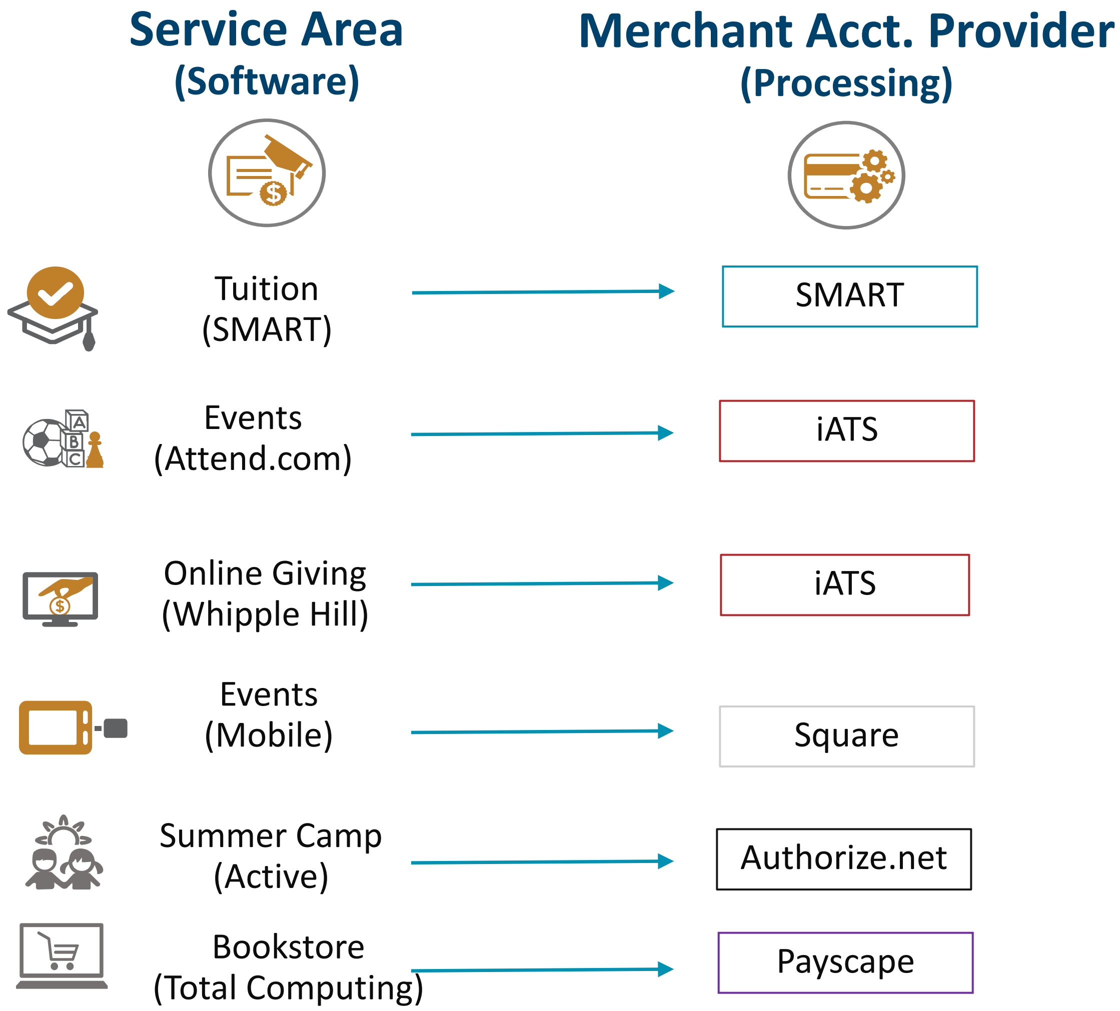
- Lost donations due to lack of or sub-optimal online giving pages
- Lost fees given up to TMCs (family fee, late fees)
- Frustrated parents (donors) due to inconvenience, poor service by third-party, high late fees

Sources: Blackbaud; Network for Good; Diamond Mind internal research

Chaos of Complexity Across Campus

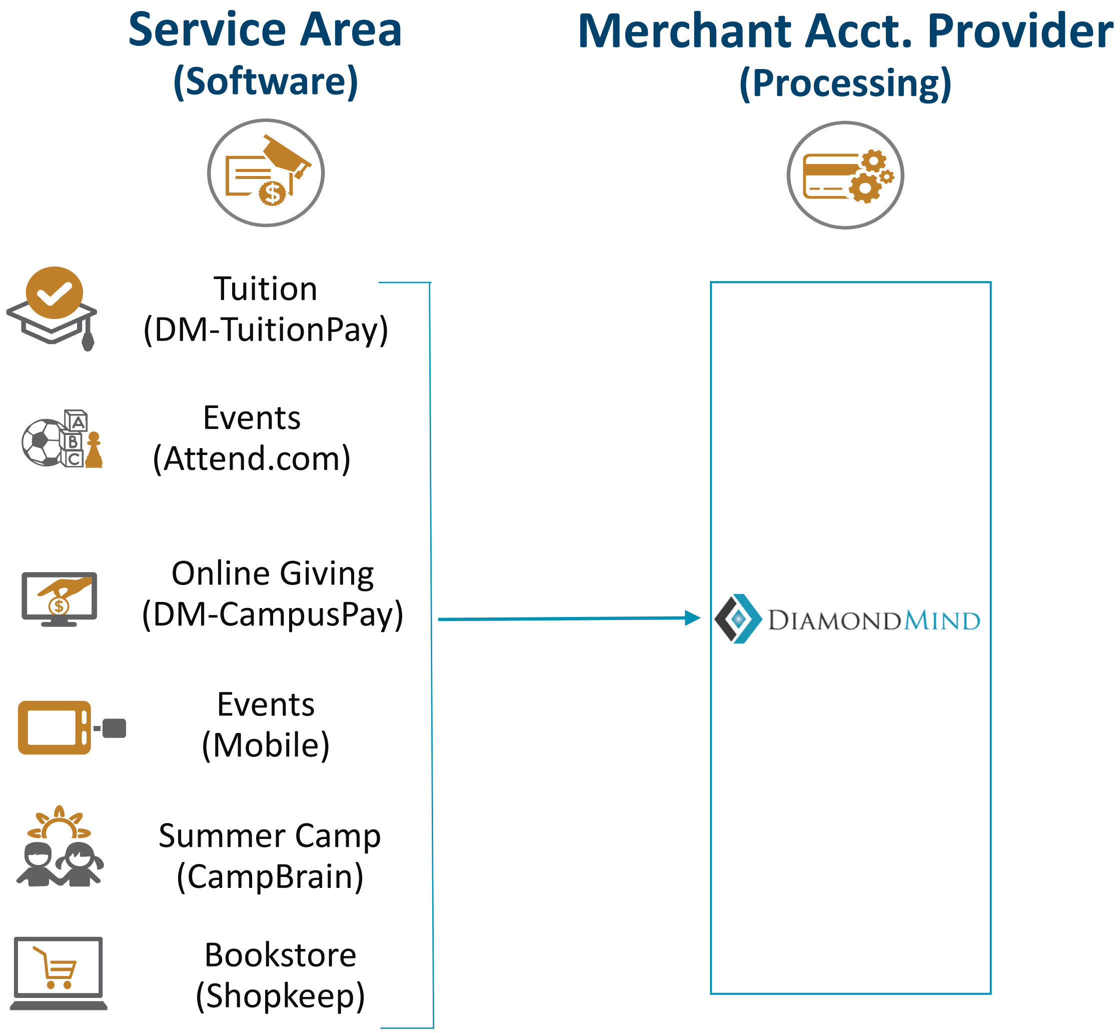
Before Diamond Mind Consolidation

- *5 Software Vendors*
- *5 Merchant Acct. Providers*
- *5 Different Payment Processing Contacts*
- *5 Different PCI Compliance Contacts*



Service Area (Software)	Merchant Acct. Provider (Processing)
Tuition (SMART)	SMART
Events (Attend.com)	iATS
Online Giving (Whipple Hill)	iATS
Events (Mobile)	Square
Summer Camp (Active)	Authorize.net
Bookstore (Total Computing)	Payscape

Chaos of Complexity Across Campus



Service Area
(Software)

Tuition
(DM-TuitionPay)

Events
(Attend.com)

Online Giving
(DM-CampusPay)

Events
(Mobile)

Summer Camp
(CampBrain)

Bookstore
(Shopkeep)

Merchant Acct. Provider
(Processing)

DIAMONDMIND

After Diamond Mind Consolidation

- *4 Software providers*
- *1 Merchant Account Provider*
- *1 Payment Processing Contact*
- *1 Contact for PCI compliance*

Benefits of Consolidation

- ✓ *Single point-of-contact*
- ✓ *Vastly simplified reconciliation*
- ✓ *Improved reporting*
- ✓ *Single statement*
- ✓ *Rate assurance*

Key Take-Aways

- ☑ Evaluate, achieve, and maintain PCI-DSS Compliance as soon as it is possible
- ☑ Have a clear plan to address areas of vulnerability
- ☑ Just because your vendors are complaint, doesn’t mean you are
- ☑ Your vendors can make achieving PCI-DSS Compliance easier or more difficult based on their status

Interested in working with the only Independent School focused Processor?

CONTACT US TODAY!

DIAMONDMIND
Payment Solutions for Schools

Contact Info:
(888) 566-0945 x777
info@diamondmindinc.com

Need More Information?

Look for other Diamond Mind educational webinars at
www.diamondmindinc.com/webinars

Visit us at

www.diamondmindinc.com

PCI Security Standards Council at
www.pcisecuritystandards.org