

E-Pay

A Case Study in PCI Compliance



**Illinois State Treasurer
Dan Rutherford**



What is PCI?

- The Payment Card Industry's Data Security Standard states:
 - PCI Data Security Requirements applies to all members, merchants and service providers that store, process or transmit cardholder data





Where Did It Start?

- **In 2000, VISA launched CISP (Cardholder Information Security Program)**
- **In 2002, MasterCard introduced its SDP (Site Data Protection) program**
- **American Express and Discover also had programs though not as robust**

Merchants had to comply with each program, making compliance virtually impossible and very costly

.....and they started complaining



Where Did It Start?

- **In December of 2004, VISA and MasterCard aligned their programs under the banner PCI Data Security Standard (PCI DSS)**
- **American Express, Discover, JCB and Diners endorsed this new standard as well**
- **VISA initially managed and coordinated the PCI DSS**
- **Card brands created the PCI Security Standards Council (SSC) to assume management of the program**
- **PCI SSC managed by Executive and Management Committees made up of senior representatives from the card brands**

End Result

Common security requirements for securing card data.

Ensuring
Merchant
Compliance

Improving Security

Mitigating Risk

Refresher for
Employees

Who Does What?



1. Develops Standards



2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)

What does the PCI SSC do?



1. Develops Standards

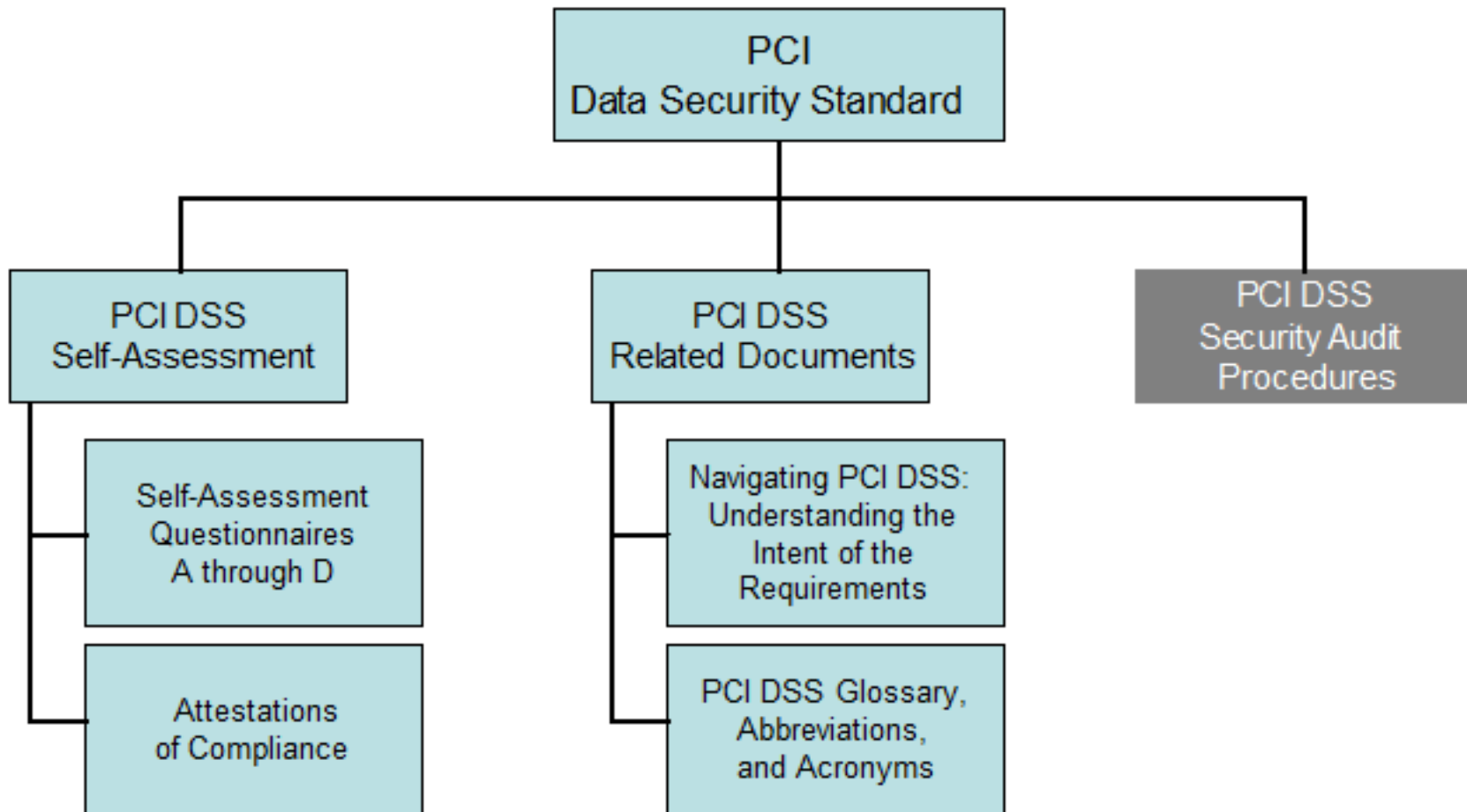


2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)

PCI Data Security Standard



What do the Card Brands do?



1. Develops Standards



2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)



They Define Merchant Levels

Level	American Express	MasterCard	Visa
1	Merchants processing over 2.5 million AMEX card transactions annually or any merchant that AMEX otherwise deems a Level 1.	Merchants processing over 6 million MasterCard transactions (all channels) annually or compromised merchants.	Merchants processing over 6 million Visa Transactions annually, identified by another payment card brand as level 1 , or merchants compromised last year.
2	Merchants processing 50,000 to 2.5 million AMEX transactions annually, or any merchant that AMEX otherwise deems a Level 2.	Merchants processing 1 million to 6 million MasterCard transactions annually or any merchant considered Level 2 by another card brand.	Merchants processing 1 million to 6 million Visa transactions annually.
3	Merchants processing less than 50,000 AMEX transactions annually.	Merchants processing over 20,000 MasterCard e-commerce transactions annually.	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually.
4	N/A	All other MasterCard merchants.	Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually.

What do the Bank's do?



1. Develops Standards



2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)



They Enforce Merchant Validation Requirements

Level	American Express	MasterCard	Visa
1	<ul style="list-style-type: none"> •Onsite Review by a QSA. •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Onsite Review by a QSA. •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Onsite Review by a QSA. •Quarterly Network Scan by ASV.
2	<ul style="list-style-type: none"> •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Onsite Review by a QSA. •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.
3	<ul style="list-style-type: none"> •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.
4	N/A	<ul style="list-style-type: none"> •Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> •Annual Self-Assessment Questionnaire •Quarterly Network Scan by ASV.



They Enforce Merchant Validation Requirements

- ✓ What you **must do**, and how you **must validate** are totally separate. (Compliance vs. Validation)
- ✓ All merchants **must be** PCI compliant at all times.
- ✓ Level 2, 3, and 4 merchants **validate** compliance through the SAQ and quarterly scans (except for MasterCard Level 2 merchants as of June 15, 2009).
- ✓ PCI DDS 11.2 requires that all merchants perform external network scanning from an Approved Scan Vendor (ASV).
- ✓ QSA stands for Qualified Security Assessor, a designation issued by the PCI SSC to firms/individuals allowing them to conduct audits and submit Reports on Compliance for Level 1 & 2 merchants and Level 1 service providers

3 Steps to Achieving PCI DSS





Six Goals - 12 Requirements



1. Build and Maintain a Secure Network

- a. Install and maintain a firewall configuration to protect cardholder data
- b. Do not use vendor-supplied defaults for system passwords and other security parameters



2. Protect Cardholder Data

- a. Encrypt transmission of cardholder data across open, public networks
- b. Protect stored cardholder data



3. Maintain a Vulnerability Management Program

- a. Use and regularly update antivirus software programs
- b. Develop and maintain secure systems and applications



4. Implement Strong Access Control Measures

- a. Restrict access to cardholder data by business need-to-know
- b. Assign a unique ID to each person with computer access
- c. Restrict physical access to cardholder data



5. Regularly Monitor and Test Networks

- a. Track and monitor all access to network resources and cardholder data
- b. Regularly test security systems and processes



6. Maintain an Information Security Policy

- a. Maintain a policy that addresses information security for employees and contractors

What's in it for the Merchant?


Improves reputation



Helps prevent security breaches
and theft



Compliance with the PCI DSS and
avoidance of non-compliance fines



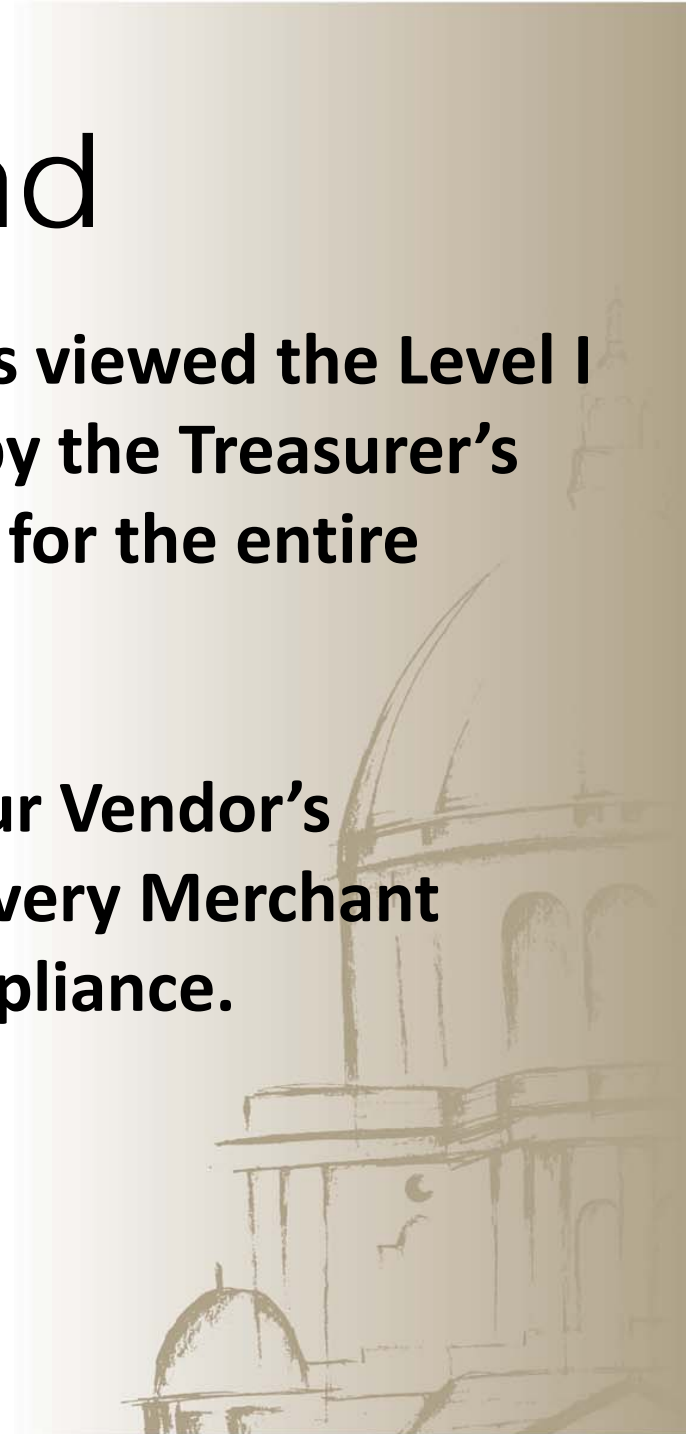
E-Pay's Challenge: Getting Participants to become PCI Compliant



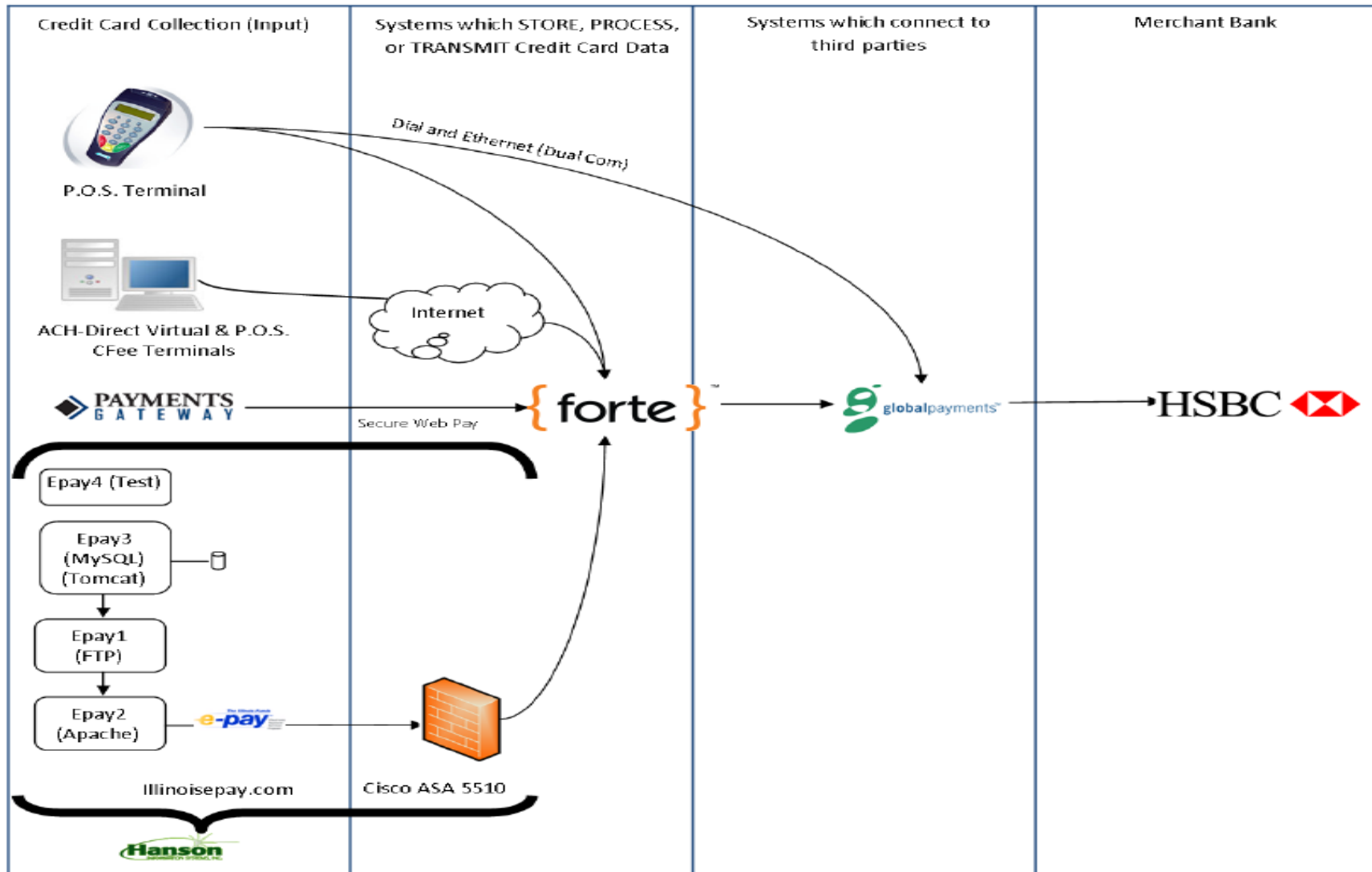
How to administer a comprehensive PCI Program to our 800+ participants—that is cost controlled, intuitive and simple enough for staff to complete?

Background

- **Until November of 2012, our Vendors viewed the Level I PCI validation completed each year by the Treasurer's Office as satisfying PCI requirements for the entire portfolio.**
- **However, in order to mitigate risk, our Vendor's sponsoring bank (HSBC) mandated every Merchant Account must have proof of PCI Compliance.**



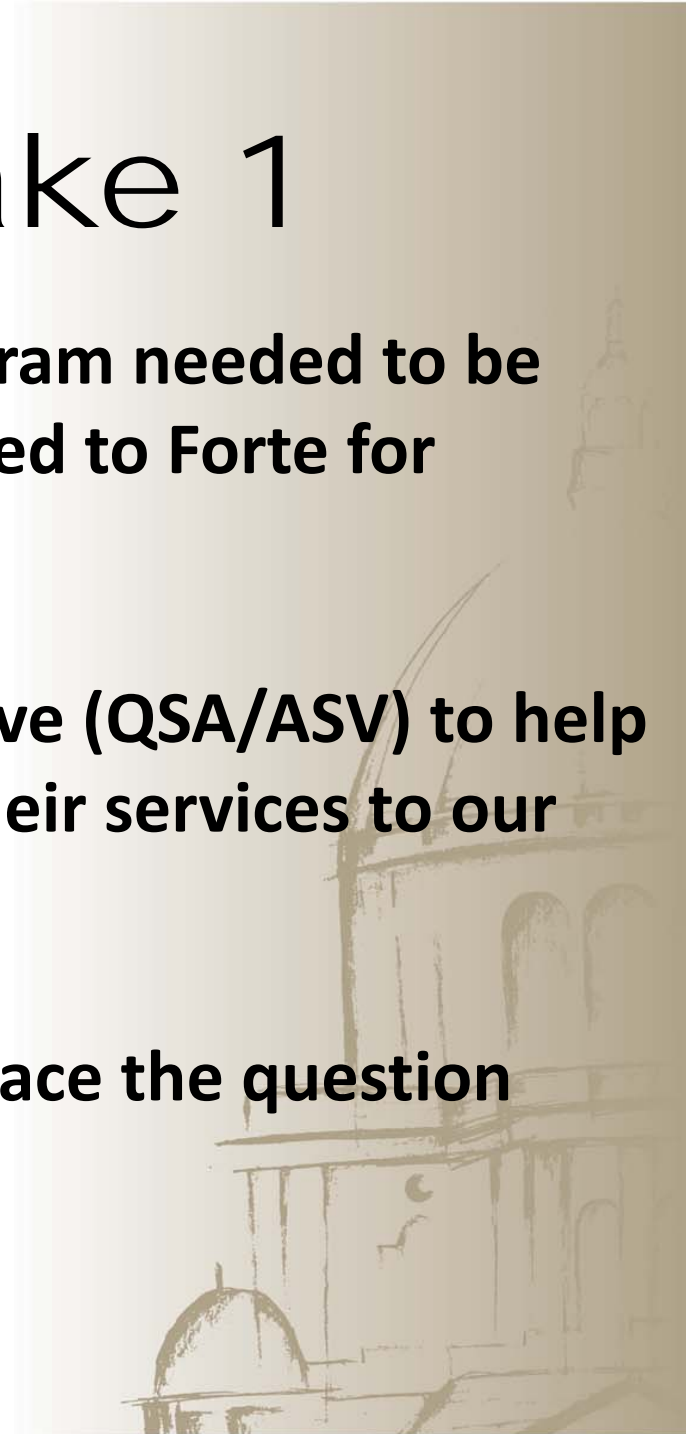
How E-Pay's Data Flows



Cardholder Data Flow Diagram

PCI Rollout: Take 1

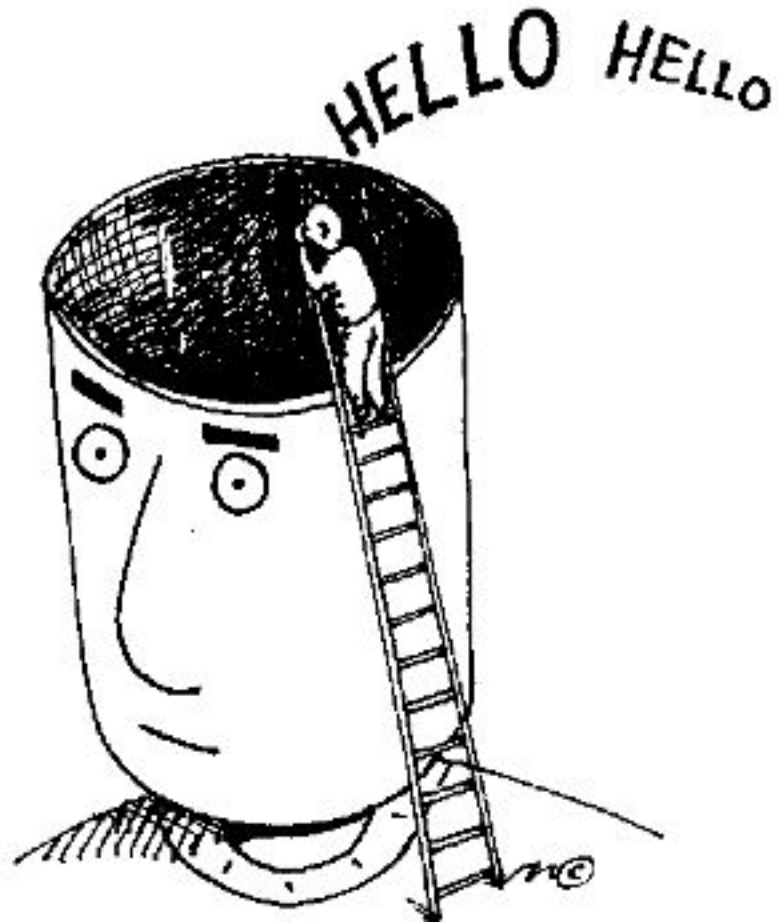
- **After learning a comprehensive program needed to be rolled out sooner than later, we turned to Forte for support.**
- **In turn, they partnered with Trustwave (QSA/ASV) to help us with our PCI Rollout by offering their services to our participants for \$7.99 per month.**
- **With the Trustwave partnership in place the question became how do we tackle this?**



PCI Rollout: Take 1

- **All non-compliant participant groups (i.e. County Treasurers, Clerks, Schools, etc.) received a pre-Trustwave communication email that was sent out in phases and included the following:**
 - Stats on small businesses**
 - Why PCI Compliance is important**
 - 3 Ways to Become Compliant (Self Assessment/Trustwave/Other QSA/ASV)**
- **Non-compliant merchants had 30 days to submit to the Treasurer's office in writing how they were going to become PCI compliant and then 90 days after to submit proof.**
- **New Participants would have to provide proof of PCI compliance before they could begin processing any payments.**

Our Response?



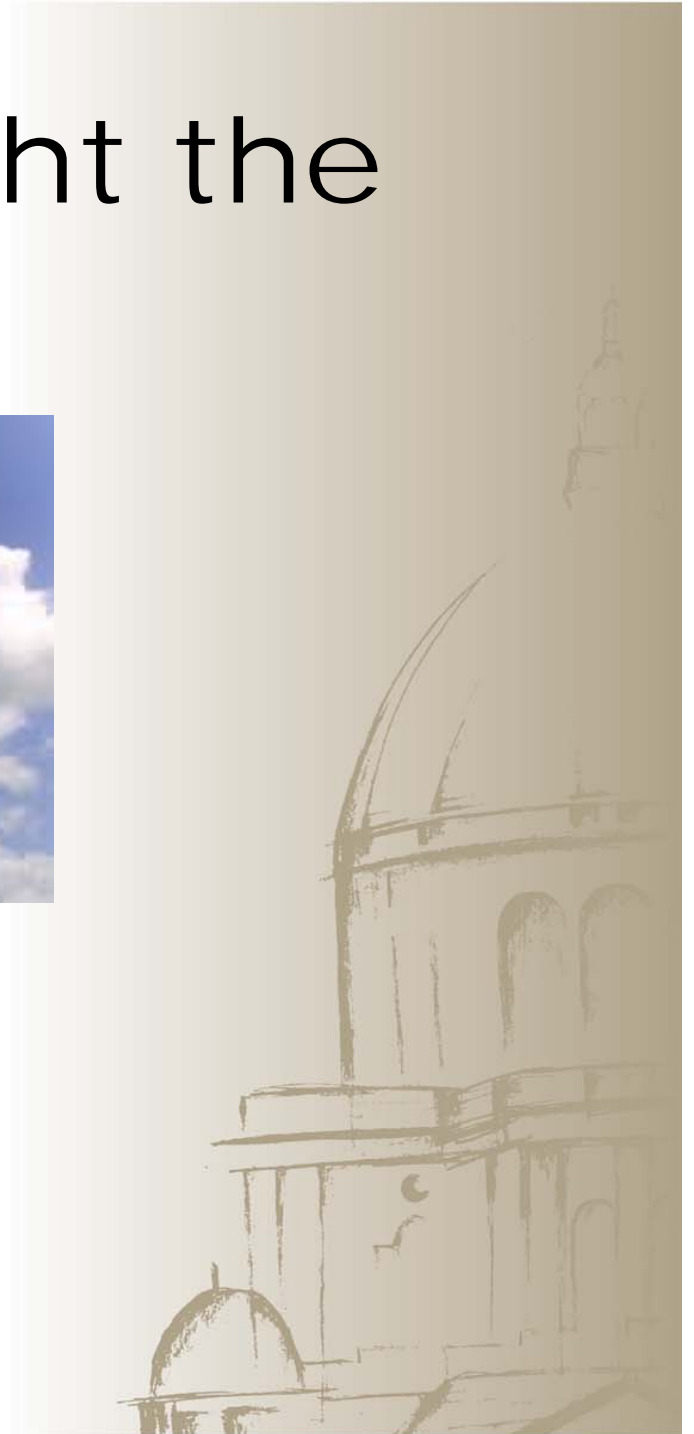
A confused participant base



What caused the confusion?

- **Participants mistook the communication as a phishing scam.**
- **Many thought that since they were such small organizations or took in little money that they did need to be compliant.**
- **Others spoke with their peers (who had different setups than themselves) about how they completed compliance and tried to apply it to their environment.**
- **Some didn't read the email or just forwarded it on to their IT team.**

How do we right the ship?

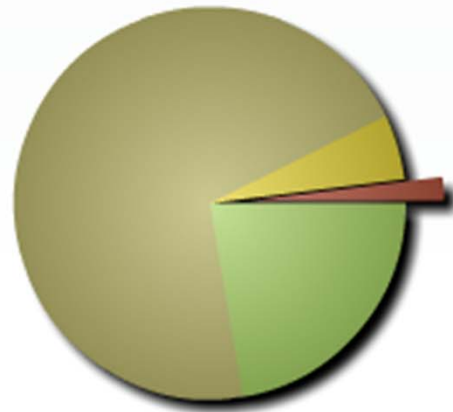


- **Started by retargeting our role out groups with more detail. Specifically, presenting them with the breakdown of their services and the options available to them. i.e. if they were internet only participants, describing the benefits of self-assessing and where to find key forms.**
- **Made sure all future releases were joint releases with E-Pay contact information for questions.**
- **Set a cut-off date whereby if compliance was not on file, they would be auto-enrolled into the Trustwave program.**
- **Since cost was prohibitive for those that required scans, Forte offered to pay for participants that were on the convenience fee model.**
- **For our state agencies, we began to work closer with the OAG's office to make sure they were aware when auditing, that this is something that must be completed.**

The results?



The results?



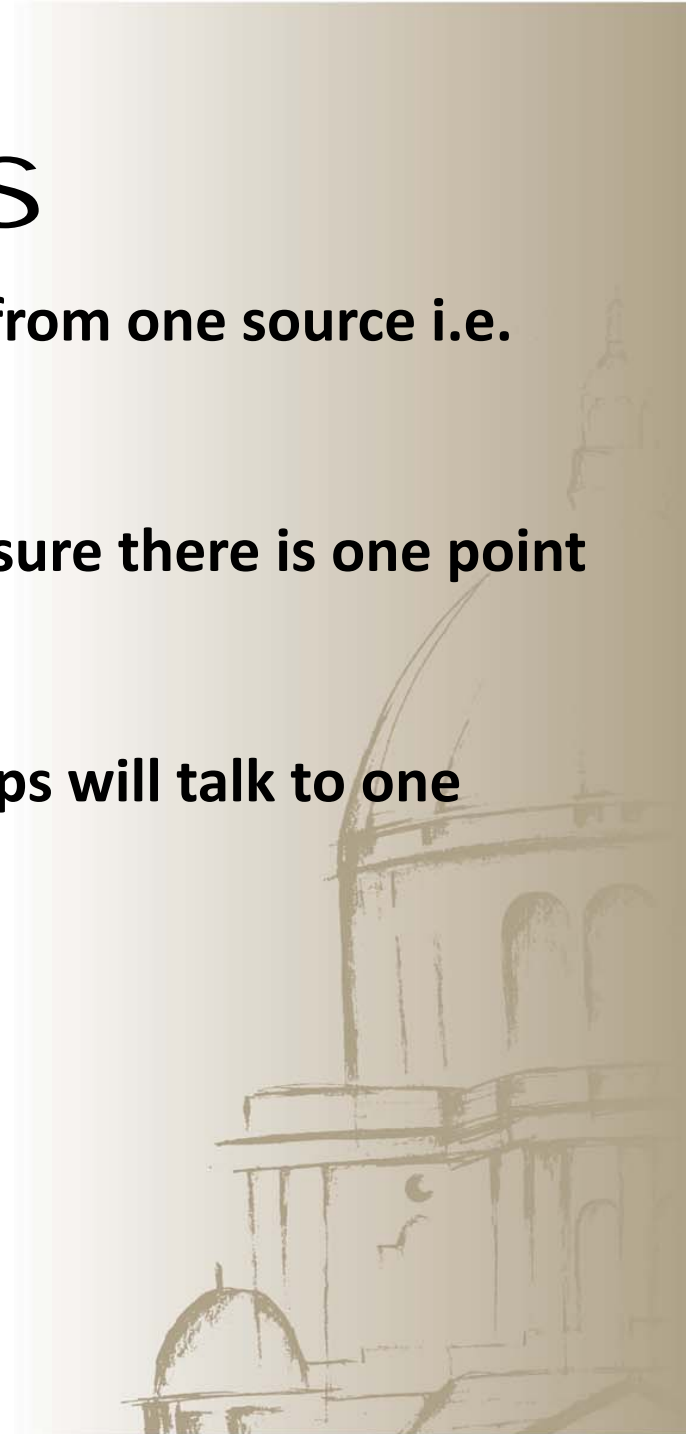
Compliance Breakdown

	Non-Compliant	<u>11</u>	(2%)
	Incomplete-Active	<u>30</u>	(5%)
	Incomplete-New	<u>394</u>	(70%)
	Expired	<u>0</u>	(0%)
	Compliant	<u>125</u>	(22%)



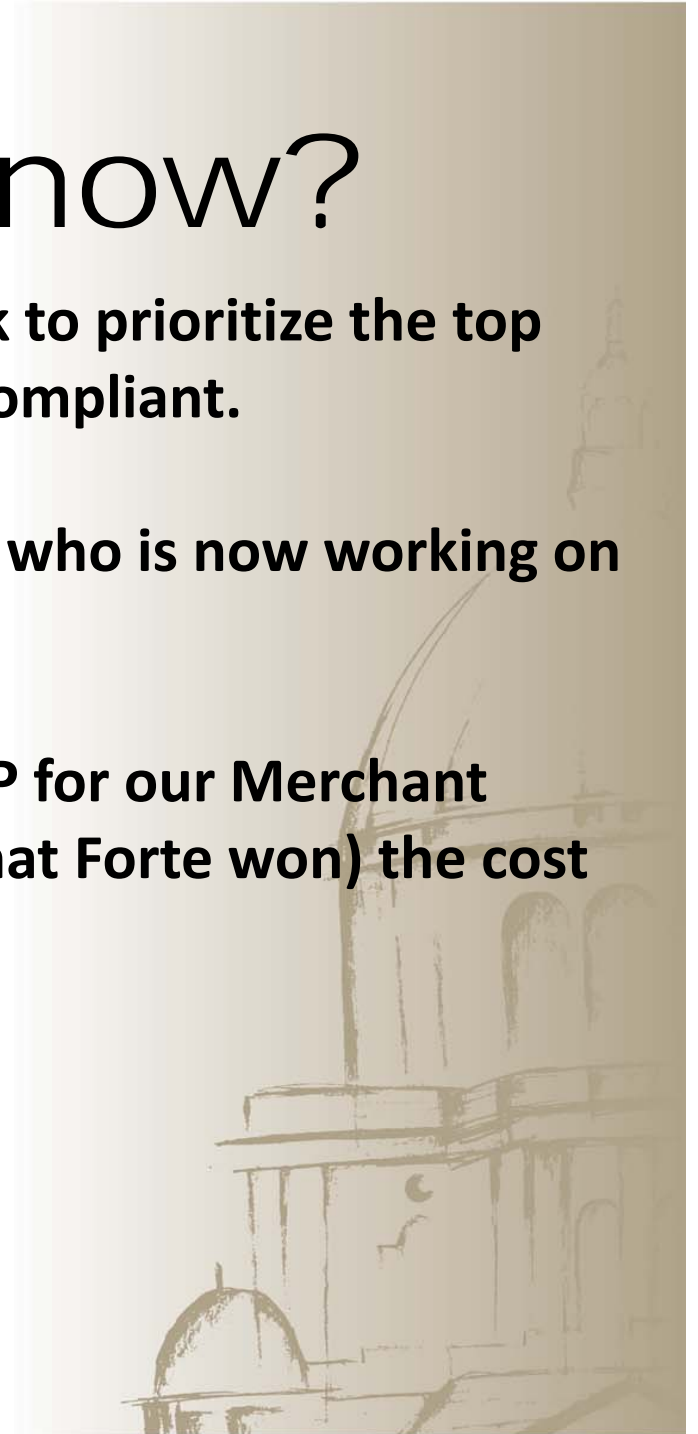
Takeaways

- **Make sure that all communications come from one source i.e. emails, notifications, etc.**
- **If dealing with a larger organization make sure there is one point of contact. Example: SOS**
- **Educate as much as possible as these groups will talk to one another. Example: webinars**



Where are we now?

- **Global asked that we (Forte and STO) work to prioritize the top 200 highest volume MIDs that aren't PCI compliant.**
- **This group includes the Secretary of State, who is now working on their own level II audit.**
- **During all of this, we had submitted an RFP for our Merchant Processing. As part of our new contract (that Forte won) the cost of PCI Compliance is paid for by Forte.**



QUESTIONS???





Contact Information

Springfield Office

The Illinois Funds
400 W. Monroe St., Ste 401
Springfield, IL 62704

Ph: 866-831-5240

Fax: (217) 524-1269

Jon Skinner – Manager of Technical Support &
Development

Email: jskinner@treasurer.state.il.us

Website: www.treasurer.il.gov

