

2011 ITS Georgia Annual Meeting

Monday, 19 September 2011

Transit IT

Part I: Legacy to Electronic Payment Systems (How to Get There)

Part II: PCI Security (Awareness)

ITS Beyond Highways



Nez Tubaya
Program Manager
Technology Infrastructure Operations
O.404.848.4312
M.202.423.5158

INVESTIGATE



What is Electronic Payment System (EPS) Technology?

- ❖ Electronic communications
- ❖ Data processing
- ❖ Data storage
- ❖ Data archiving/retrieval
- ❖ Data Security - Payment Card Industry Data Storage Standard (PCI DSS) - As a merchant if you store cardholder data in any way, shape, or form you are required to maintain that information in a secure manner

What else do we need to know?

INVESTIGATE

- ❖ HW/SW Procurement
- ❖ SW Licenses & Fees
- ❖ Maintenance Agreements
- ❖ Computer & Network Resource Usage

Active U.S. Transit Smart Card Projects and Implementations

(Re: Smart Card Alliance Link) <http://www.smartcardalliance.org/pages/smart-cards-applications-transportation>

INVESTIGATE

- ❖ [Atlanta/MARTA Breeze Card](#)
- ❖ [Boston/MBTA Charlie Card](#)
- ❖ [Chicago/CTA \(Chicago Card and Chicago Card Plus\)](#)
- ❖ [Houston/METRO](#)
- ❖ [Las Vegas/Monorail](#)
- ❖ [Los Angeles/LACMTA \(UFS\)](#)
- ❖ [Maryland Transit Administration \(MTA\)](#)
- ❖ [Miami-Ft. Lauderdale-Palm Beach/MDTA/SFRTA \(UAFC\)](#)
- ❖ [Minneapolis-St. Paul/Metro Transit](#)
- ❖ [MTA/New York City Transit pilot](#)
- ❖ [Newark/PANYNJ & NJT \(SmartLink\)](#)
- ❖ [Orlando/Lynx \(ORANGES\)](#)
- ❖ [Port Authority Trans Hudson \(PATH\)](#)
- ❖ [Philadelphia/PATCO](#)
- ❖ [San Diego/MTDB](#)
- ❖ [San Francisco/MTC \(Clipper Card\)](#)
- ❖ [Seattle-Puget Sound/KC Metro ORCA Card](#)
- ❖ [Utah Transit Authority](#)
- ❖ [Ventura County](#)
- ❖ [Washington Metropolitan Transportation Authority SmarTrip](#)

Lessons Learned 1: Take the time to become more informed...

INVESTIGATE

- ❖ Understand the implications of the EPS attributes
- ❖ Contact Transit Agencies with EPS technology already in place
- ❖ Realize through peer communications the concepts that are similar and those that are vastly different
- ❖ Determine next steps for your new business model

COMMUNICATE

- ❖ Who or what is driving the technology changes in transit?
- ❖ Where can the relative information be found?
- ❖ How are communications established internally / externally?

Is IT Really Driving?

COMMUNICATE

- ❖ IT is the conduit for services between and among stakeholders
- ❖ IT is the conduit for securing data connections, transmissions, and data archiving/storage
- ❖ IT is the conduit for manipulating valuable data for reporting
- ❖ IT is driven by customer requirements

Lessons Learned 2: Acknowledge that the resources are limited and you will need to encourage your team to enhance their skills.

Now you need to find out how much your IT resources understand the new technology, and if they can do the work to support the migration and implementation!

IT resources are literally constrained
by the numbers

of Dollars vs. # of Retainable/Obtainable Resources

How do you accomplish this effort with fewer and less skilled resources?

Lessons Learned 3: Identify Resource Challenges and Skill Requirements, then Measure and Manage the Team's Efforts

COMMUNICATE

Internal Resource Challenges

- Determine who is available within your organization
- Determine from the availability who has the ability to manage and/or support a new system
- Determine who has the best communications skills

Co-Create Experiences with your Team

- Encourage an active dialogue between team members
- Manage team diversity
- Cultivate multiple channels of experiences
- Allow more autonomy to managers

Lessons Learned 4: Manage and create value added

Value Added by Managers

- Nurture and build competencies
- Manage collaborative partnerships
- Harness competence
- Manage personalized experiences
- Shape customer expectations

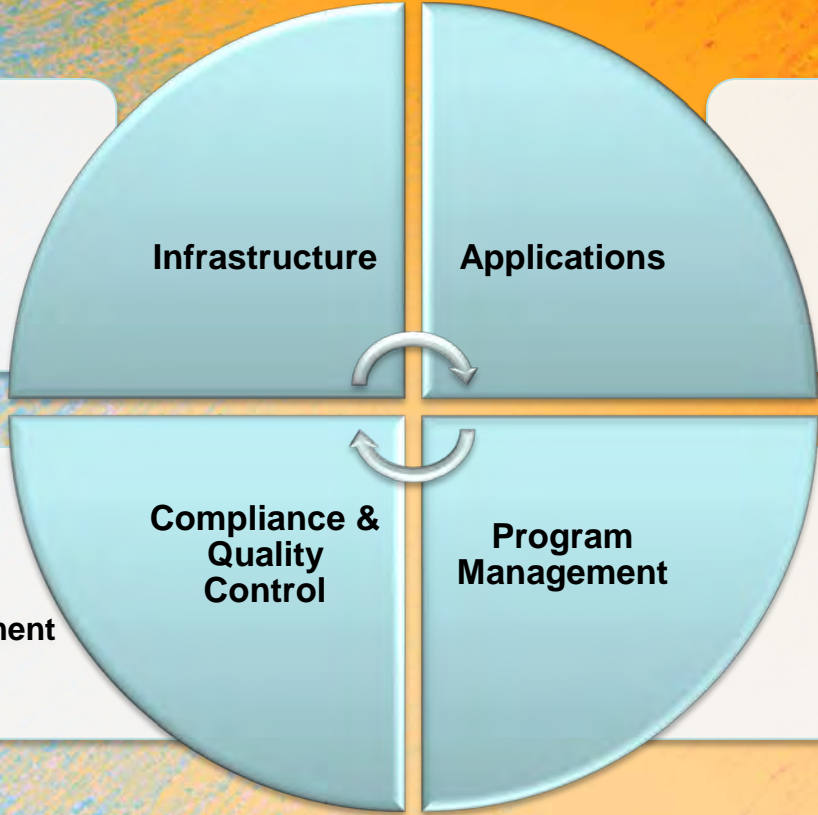
Value Creation

- Autonomy
- Collaborate with partner companies
- Collaborate with partner companies and with active customers
- Implement resource skill rotation programs
- Implement of manager skill rotation programs

Implement a Resource Rotation Program

COMMUNICATE

- NetOps
- SysOps
- Telephony
- Help Desk
- NOC/Data Center
- Security



- Data Warehouse
- Information Systems
- Software APPs
- Security

- Quality Assurance
- Quality Control/Audit
- Configuration Management
- Security

- Portfolio Management
- Programs/Projects
- Business Processes
- Contracts/Procurement

Lessons Learned 5: Identify Internal Resource Challenges and Skill Requirements, then Reach to Outside Sources

External Resources – *Maintains the internal knowledge base*

- Reach out to other Transit Authorities via Peer Reviews or Site Visits
- Identify Resources within your Public Network

Outsourcing - *Minimizes the internal knowledge base*

Lessons Learned 6: Identify Technology Challenges and Resolve them Internally

Workplace technology is constantly evolving. Acquiring specialized skills and knowledge, and staying current in computer software and new programs, can make or break opportunities to forge ahead with new technology initiatives. We all should understand that we are limited when it comes to always knowing who moved the cheese.

Let your team assist you in identifying the changes in technology. The most common way to get your team involved is to encourage them to conduct research via the internet or attend relative social networking events. Learning will do more than provide practical skills for work, but rather place them in a position to teach others; therefore keeping the knowledge in-house. It will also boost their self-esteem and supply an added dose of much needed confidence when presented with a new technology project. This effort will also minimize the knowledge transfer time.

COMMUNICATE

INTEGRATE

What do we need to know in order to integrate EPS technology into a legacy environment?

Integrating new technology into your legacy world is not going to be simple...

INTEGRATE

So you have successfully scaled back on your resources and saved the Authority loads of money. You are then directed to integrate a new EPS technology into your legacy world.

Unfortunately, you have just realized that the effort to integrate new technology is much more than just a notion. It requires a significantly greater amount of IT support than your existing legacy revenue collections systems.

This is the point where it becomes imperative that you assess and address all aspects of your proposed business requirements with the stakeholders. Integration requires something to change. **In this case it is your business model.**

Lessons Learned 7: Approach to Change

This presentation has been cumulated from a 'lessons learned' approach. It is based on actual transit legacy to smartcard implementation business practices used by MARTA IT, and has proven to be very effective. Learning about what you already have and why you have it will help you qualify what you need in order to get what you want. Assess, address and develop your new business model before introducing anything new into your transit world.

Evidence of a technological change is coming to transit

STATISTICS

- **APTA / Trans/Tech**
- **SCA**
- **FTA**
- **TAG**
- **MIT**

...and other analytical or research organizations have documented statistical data that supports the theory that a technology change in transit is inevitable.

Lessons Learned 1: Take the time to become more informed...

Lessons Learned 2: Acknowledge that the resources are limited and you will need to encourage your team to enhance their skills.

Lessons Learned 3: Identify Resource Challenges and Skill Requirements, then Measure and Manage the Team's Efforts

Lessons Learned 4: Manage and create value added

Lessons Learned 5: Identify Internal Resource Challenges and Skill Requirements, then Reach to Outside Sources

Lessons Learned 6: Identify Technology Challenges and Resolve them Internally

Lessons Learned 7: Approach to Change

PCI Security Awareness



Warren Bridges, MIS, CQA, CICP
Technical Architect
Technology Information Security
O.404.848.4311
M.770.315.6924

MARTA HQTRS
2424 Piedmont Rd., NE
Atlanta, GA 30319

Overview

- **The Importance of PCI-DSS**
- **MARTA's PCI Compliance Relationship**
- **MARTA's PCI Goals and Requirements**
- **Employee and Partner Responsibilities**



PCI-DSS – Payment Card Industry Data Security Standards

The PCI standard states that any merchant who stores, processes or transmits payment cardholder data must protect credit card information from accidental disclosure



PCI Protection



PCI provides protection for all participants in a credit card transaction:

- **The Cardholder (MARTA Patrons using Credit/Debit)**
- **Merchant (MARTA, Regional Partners such as GRTA, CCT, and GCT)**
- **Banks/Acquirers (Bank of America)**
- **Service Providers (Cubic)**
- **Card Brands (Visa, MasterCard, American Express, Discover)**



Why Is PCI Compliance Important?

- Demonstrates MARTA's commitment to protecting customer's confidential data.
- Indicates stronger controls & processes which help to prevent the risk of data compromises
- Avoid substantial fines and penalties from the credit card industry



When Data is Breached



Data breaches can lead to significant adverse consequences

For MARTA:

- Unwanted media attention
- Lost revenue and/or financial damages
- Litigation
- Substantial VISA and MasterCard penalties
- Loss of customers' trust

When Data is Breached (Cont'd)

Data breaches can lead to significant adverse consequences

For the Patron/cardholder:

- Identity theft
- Unauthorized charges to their credit or debit card account
- Damage to their personal credit rating
- Financial losses

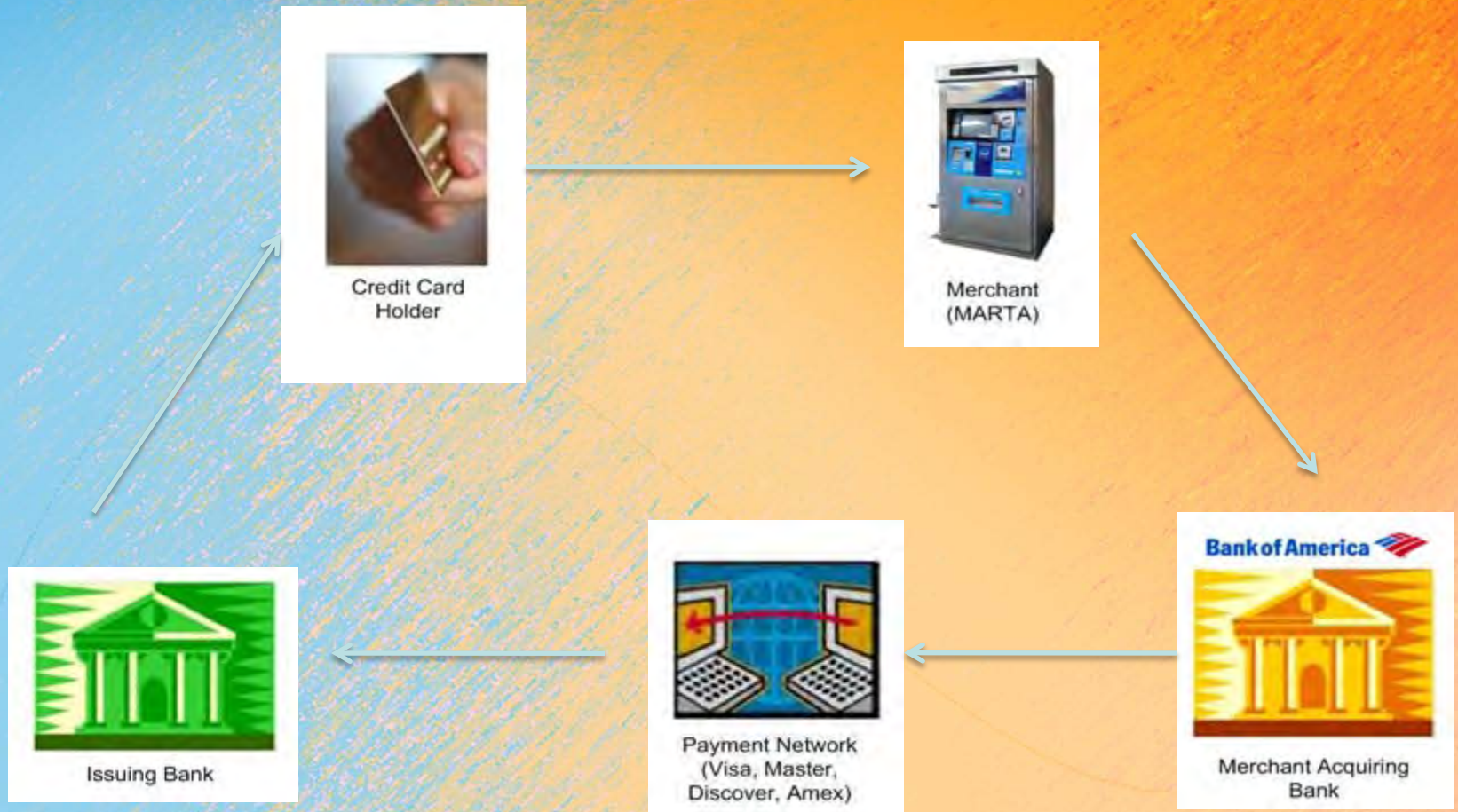


MARTA's PCI Compliance Relationship



A Typical Credit Card Transaction

A typical credit card transaction





How MARTA Remains Compliant



Note: MARTA processes between 1 to 6 million credit card transactions annually and has been defined as a Level Two Merchant

- MARTA has validated that all PCI requirements meet compliance
- MARTA has completed the Annual Self-Assessment Questionnaire (SAQ)
- MARTA has provided Quarterly network scans by an Approved Scan Vendor (ASV)
- Marta has completed the Attestation of Compliance Form

MARTA PCI Compliance Responsibilities



Store, Process or Transmit

Anyone who “**Stores, Processes or Transmits**” cardholder data must comply with the PCI-DSS standards, and MARTA’s PCI –DSS applies to:

- Business Partners (Banks & Acquirers – Bank of America, Regional transits)
- Service Provider (Cubic)
- MARTA AFC Network infrastructure
- Applications & Databases (Nextfare, Hummingbird, EFT)
- Devices (Point of Sale (POS) TVM, TOMs, Parking meters)



PCI Protects.....



The cardholder's identity and confidential data, including:

- Magnetic stripe (track 1 and track 2 data)
- Card Verification Values (CVC, CVV2 – 3 or 4 digit codes printed on back or front of card)
- Payment Account Numbers (PAN)
- Personal Identification Numbers (PIN)
- Card expiration dates



MARTA's PCI Goals and Requirements



Six Main Control Areas of PCI



- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy



Employee and Partners Responsibilities



Working in Information Technology

Remember to:

- Never store magnetic stripe, CVC2 or PIN data after authorization.
- Don't use administrator accounts to perform regular user tasks.
- Ensure that all non-console administrative access is encrypted. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.



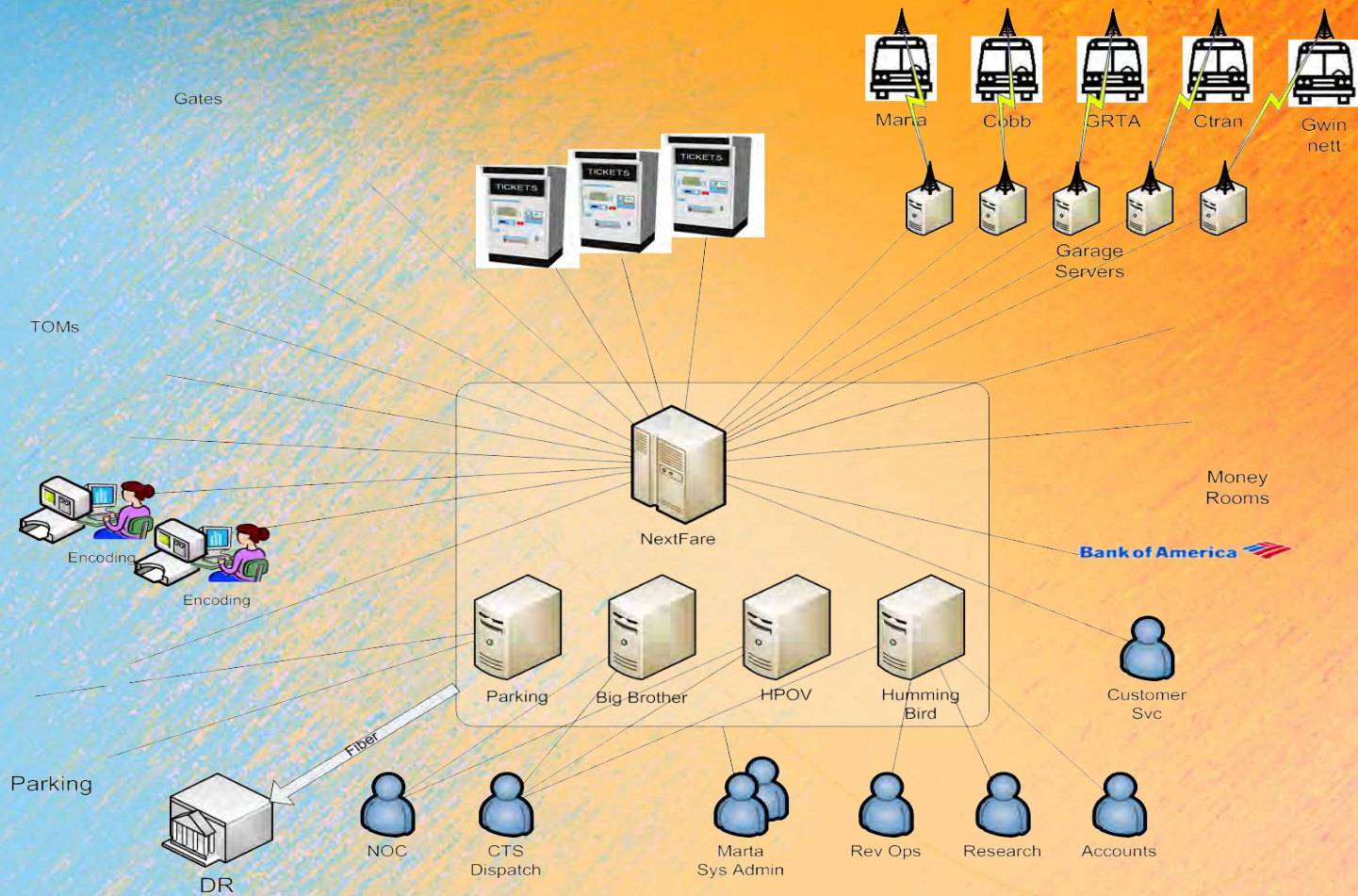
Working in Information Technology (Cont'd)

Remember to:

- Restrict physical access to payment card data or systems storing card data.
- Protect and manage backup media. Store media securely, log removal of media, transfer securely, and destroy securely according to the data retention policy.
- Complete annual security awareness training.



MARTA AFC System



QUESTIONS?



Ben Graham, MA, MBA
Technology AGM/CIO
O.404.848.4075
M.404.493.2364

MARTA HQTRS
2424 Piedmont Rd., NE
Atlanta, GA 30319