

January 23, 2008

Field Processing of Credit Cards: Solving Credit and Collections Issues

Robert Sarfi

RSarfi@BoreasGroup.us
(720) 220-6213

Roger Schneider

Roger.Schneider@smeco.coop
(301) 274-4317

Mike Tao

MTao@BoreasGroup.us
(720) 635-8347

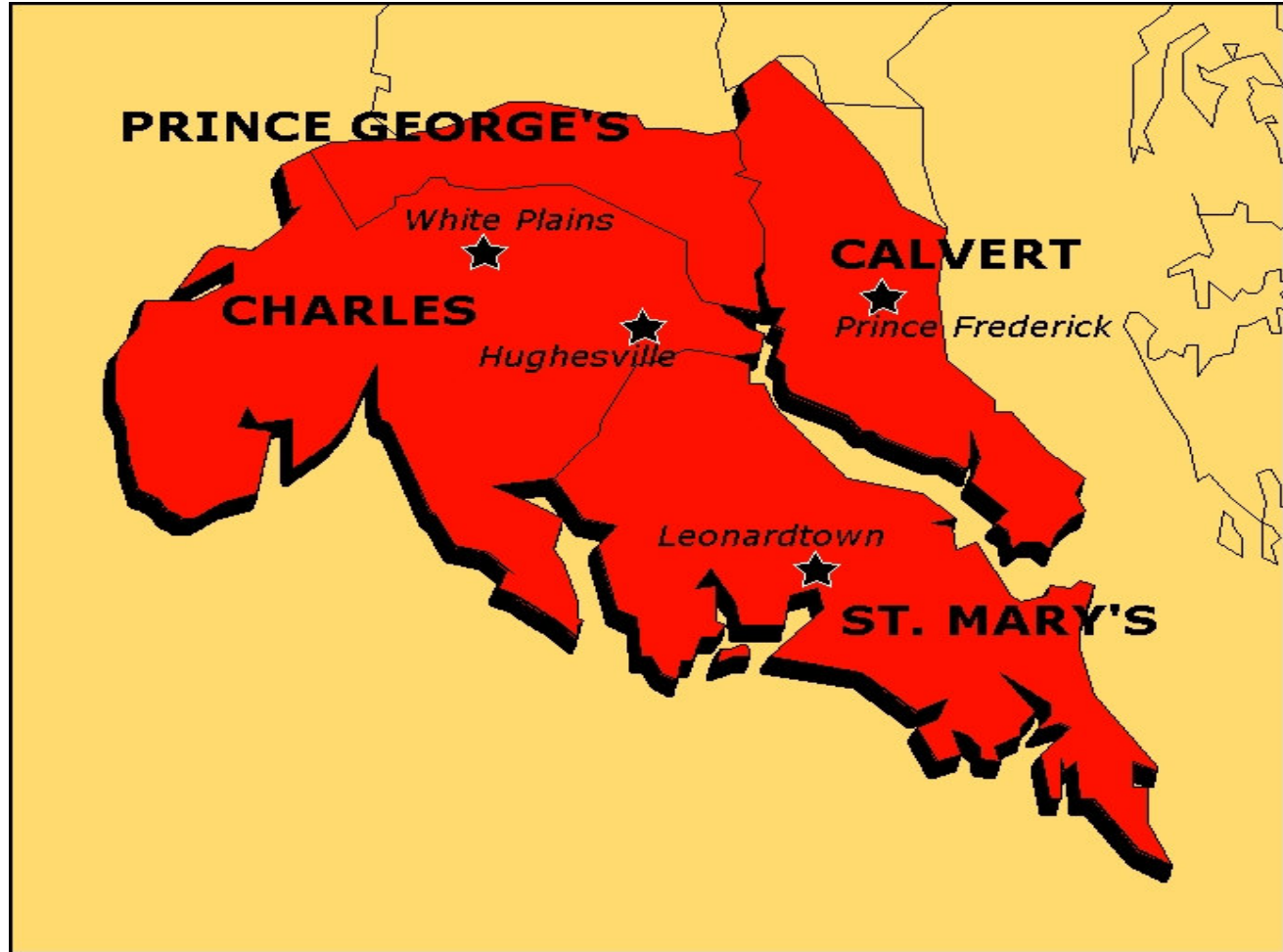
Thomas Bannon

Tom.Bannon@chasepaymentech.com
(214) 849-2179

(240) 528-9749



About SMECO



Agenda



1. Introduction
2. Cost / Benefit Considerations
3. Compliance Requirements
4. Options
5. Summary

1. Introduction



Field Credit Card Processing

- Utilities are pressured to adopt commonly accepted payment practices available to society as a whole
- Most merchants and vendors interacting with retail customers accept credit cards
 - 92% of retail vendors / merchants accept credit card payments
 - 48% of utilities accept credit cards
 - 35% of electric utilities accept credit cards
 - 15% of electric utilities accept field credit card payments
- Customer service opportunities abound for utility acceptance of credit card payments
 - Delinquent account payments
 - Customer contribution in aid of construction
 - Service visits
 - Appliance installation and repair.

Utilities are Intimidated by Accepting Credit Cards in the Field

- Do not appreciate value of card acceptance
- Desire to separate field resources from collection of money
- Ability of customers to contest or reverse charges
- Overall security considerations
- Lack of understand of infrastructure requirements
- Adversity to change

***While these perceptions have merit and should be addressed,
utilities miss a strategic opportunity in not accepting card payments.***

Benefits of Card Acceptance

- Favorable image
 - Consistent with current societal trends
 - ie communications companies and other service providers
- Guaranteed payment upon transaction authorization
- Reduction in credit and collections costs
 - Reduction and potential elimination of NSF check fees
- Elimination of cash and check collection by field resources
- Receipt of guaranteed payment within 24 to 48hours

As with any other change a utility must quantify and balance cost / benefits.

Costs Associated with Card Acceptance



- Processing fees vary considerably
 - \$0.05 to \$4.00 per transaction
- Cost of transaction influenced by many factors
 - Credit risk associated with target consumers
 - Transaction volume
 - Special services
 - Individual transaction size
 - Level of service / provider
- Numerous options exist for card processing
 - Direct i.e. major card processing firm, such as Chase Paymentech
 - Independent Service Organization (ISO) is typically a regional distributor that buys services of a major organization and bundles
 - Value Added Reseller wraps processing services within software application or service targeted at a specific industry
- Infrastructure requirements
 - Wireless communication
 - Hardware
 - Integration
 - Security, in particular PCI DSS
- Societal impact
 - In some jurisdictions there is a feeling that consumers cannot manage credit

Security and PCI compliance must be taken seriously.

3. Compliance Requirements

Understanding PCI Compliance



What is PCI DSS



- PCI DSS is a standard to combat card related fraud:
 - Mail/Internet order fraud;
 - Account takeover;
 - Skimming; and
 - Carding.
- Driven by Visa, MasterCard, American Express, Discover and JCB to standardize on a common set of data security requirements for merchants and data processors.
 - Council formed in 2004
 - Independent organization to promote card security
- Version 1.1 of the PCI DSS standard was published in September 2006.
 - Compliance is a requirement of all agreements in place to accept credit cards.

Either directly or indirectly PCI is applicable to anyone who accepts credit cards.

PCI Compliance Considers



- File and Disk Level Encryption
- Enterprise and Personal Firewalls
- Ongoing Vulnerability Testing
- Intrusion Detection Systems
- Internal Modem Control
- Operating System File Integrity
- Web Site Security
- Wireless Security
- Platform Security Compliance
- Remote Security Administration
- Remote Access Authentication/Identity Management
- Self-Service Password Reset
- Log Analysis and Consolidation
- Network Traffic Monitoring and Reconstruction
- Forensic Investigations and Media Analysis
- Self-Audit
- External Audit
- Intrusion Prevention (Behavioral).

PCI compliance dictates the level of risk that a utility can tolerate and prescribes very specific self and external audit guidelines.

PCI Requires



- Build and Maintain a Secure Network
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
 - Maintain an Information Security Policy
 - Requirement 12: Maintain a policy that addresses information security

This represents greater effort than most utilities current consider.

Does PCI DSS Apply to Me?

- PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed or transmitted
- PCI DSS security requirements apply to all “system components” – defined as “any network component, server or application that is included in or connected to the cardholder data environment”
- If a PAN is *not* stored, processed or transmitted then PCI DSS requirements *do not* apply.

1) Simple non-compliance can result in penalty of \$500k.

2) One time fraud does not necessarily result in PCI DSS penalty.

3) A breach that is the result of non-compliance results in double-penalties!

4. Options



A large central area with a light blue background, featuring a series of thin, light blue lines on the left side that resemble a stylized sawtooth or zigzag pattern, and a series of thin, light blue horizontal lines on the right side, resembling a ruler or scale.

Implementation Options



- Card not present transaction (CNP)
 - Low implementation cost
 - Requires no more than mobile phone
 - Requires manual transaction record
 - Highest transaction cost
 - Lowest security risk
- Third party wireless (standalone)
 - Low implementation cost
 - Hardware cost factored into transaction cost
 - Requires manual transaction record
 - High transaction cost
 - Low security risk
- Third party processing via virtual terminal
 - Low implementation cost
 - Relies on preexisting MWM implementation
 - Requires manual transaction record
 - Lower transaction cost
 - Moderate security risk
- Integrated Wireless via Internet Transport
 - Highest implementation cost
 - Relies on preexisting MWM implementation
 - Automated transaction recording
 - Lowest transaction cost
 - Highest security risk



5. Summary



Things to Consider



- Identify need
 - Review both tangible costs and benefits
 - Consider customer service factors
 - Make credit card go / no-go decision

- Identify, review, and assess implementation requirements
 - Options
 - Hardware / software / communications
 - Compliance requirements, initial and ongoing
 - Process implications
 - Negotiate favorable commercial agreement with provider
 - Perform risk analysis

- Implement

Improved customer satisfaction -> Favorable consideration by regulators!

6. Discussion

**Robert Sarfi**

RSarfi@BoreasGroup.us
(720) 220-6213

Mike Tao

MTao@BoreasGroup.us
(720) 635-8347

Roger Schneider

Roger.Schneider@smeco.coop
(301) 274-4317

Thomas Bannon

Tom.Bannon@chasepaymentech.com
(214) 849-2179

(214) 598-9749

CONFIDENTIAL