

 <p><b>MISSISSIPPI MANAGEMENT &amp; REPORTING SYSTEM</b></p> <p>Meeting the Management Information Needs for the State of Mississippi</p>	<p><b>MMRS Agency Portal Update Meeting Session Minutes (November 30, 2007)</b></p>
<p><b>Presenters: Cille Litchfield (DFA), Renee Murray (ITS)</b></p>	
<p><b>Purpose of Meeting</b></p>	
<p>This meeting was designed to bring agency users up to date on what is happening within the Department of Finance and Administration (DFA) and the Department of Information Technology Services (ITS) regarding the acceptance of credit/debit card and e-check payments online or in person.</p>	
<p><b>Status of RFP 3501 and Bank of America Agreement</b></p>	
<p>Our objective with the RFP 3501 (Bank of America (BoA)) was to engage in a full-meal array of credit card, ACH, point-of-sale (POS) and related services. The State was seeking an enterprise solution that would give us significant improvements in pricing; single vendor contact; and make comprehensive use of the existing settlement back end.</p>	
<p>What we discovered were the following:</p>	
<ol style="list-style-type: none"><li>1. There is no "one answer" for card (merchant services) + e-check/ACH (treasury services) within the banking industry.</li><li>2. Every one who deals with VISA/MasterCard has a different opinion of the "rules".</li><li>3. Just because it makes sense to do things a certain way does not mean that the card associations agree.</li><li>4. Card associations do not see government as having needs and requirements that differ from the commercial sector.</li><li>5. Liability is a huge issue and the Payment Card Industry Data Security Standard (PCI DSS) is the standard that is going to be enforced. The card associations are not concerned about the State's Constitutional limitation on liability.</li><li>6. While there are some issues, our existing approach is a sound and workable solution overall.</li><li>7. Completing a migration to the BoA product set would have pushed us back and was not a sound business decision.</li></ol>	
<p><b>Short Term Solution</b></p>	
<p>Our short term solution is to continue our Agreement with ChoicePoint Government Services (CP), at least through the end of the current contract extension of September 1, 2008. It is the final extension authorized for this Agreement, although we have discussed the possibility of additional extensions with CP and ITS..</p>	
<p>The CP solution allows us to:</p>	
<ol style="list-style-type: none"><li>1. Maintain our current processes while assessing our PCI DSS compliance status;</li><li>2. Add AMEX as an option to our existing applications and for new applications;</li><li>3. Place new portal based payment applications in the queue for deployment.</li></ol>	
<p>There are "mixed messages" from the card associations regarding:</p>	
<ol style="list-style-type: none"><li>1. Virtual Terminal Point of Sale (POS) – Can you do it as a counter application with a card swipe/direct entry and use the card not present fee structure (same as the web)</li></ol>	

without increasing the liability? Is this allowed at all? This issue continues to be researched, but it seems every one you ask has a different opinion.

2. EOC fee - This must be split from the convenience fee and displayed as a separate entry on the customer receipt. This is in direct violation of the card association convenience fee rules and we are discussing how to address this matter.
3. The calculation of the convenience fee – One issue is percentage (way the “Charges Client” works today) vs. sliding scale. Another issue is whether you have to charge the same convenience amount for anything sold within a single application. This continues to be researched.
4. Credit Card vs. e-Check Fees - Should the convenience fee be the same for both type payment transactions? Currently they are not. The credit card convenience fee is calculated on a percentage basis and the e-check is a set fee. Are we in violation of some rules as we do this?

It should be noted that the existing [electronic payment administrative rule](#) (PAYMENT BY CREDIT CARD, CHARGE CARD, DEBIT CARDS OR OTHER FORMS OF ELECTRONIC PAYMENT OF AMOUNTS OWED TO STATE AGENCIES) currently allows agencies to pay the actual processing costs for their payment transactions; some agencies possibly will want to explore this.

Traditional point of sale is not supported by CP. If it can be determined that the virtual terminal approach is acceptable, this approach is supported and in use today at the Department of Health in their clinics.

### **Long Term Plans**

#### **Merchant Cards Incident Security Plan**

1. DFA and ITS are currently working on an RFP for Payment Card Industry Data Security Standard (PCI DSS) compliance audits, training, and remediation. This is in the ITS review cycle and should be ready for advertisement in early January 2008.
2. There will also be inter-agency agreements that shift liability based on operational options:
  - a. ITS hosted application
  - b. Self-hosted application
  - c. 3rd party hosted application.

The administrative rule (referenced earlier) will be updated to include changes related to fee structures (remove EOC from the convenience fee picture, as well as other model changes) and will address the PCI DSS issues/requirements. The rule changes will also reflect requirements related for risk mitigation and additional requirements related to the Incident Security Plan.

Other items we need to determine include:

1. Whether to upgrade to ChoicePoint's Hosted Forms. This is similar to a PayPal or Official Payments type payment service. The customer would leave the agency application and be directed to a payment interface that resides within the ChoicePoint environment. This would reduce some of the PCI DSS compliance requirements for the Agency/ITS, since the card holder data would not be transferred within the State's environment (currently is a known PCI DSS issue).
2. Whether we should redefine the requirements and issue a new RFP for payment services.

### **Agencies with 3rd Party Applications**

Agencies with 3rd party applications should immediately:

1. Determine the PCI DSS certification of your vendor;
2. Understand, via your contract, who is liable in the event of a breach and take appropriate action to ensure that the State is protected; and
3. Make sure your staff understand what is expected of them when handling bank account and card holder info, etc.

The requirements regarding 3<sup>rd</sup> Party Applications will be expanded in the proposed Incident Security Plan, but agencies should start review of existing agreements and procedures immediately.

### Legislative package

[Agency Portal Update Meeting Handout](#)

### Questions and Answers

**Q:** Libby Cajoleas (Secretary of State's Office)

They still have the PCI DSS self assessment questionnaire and wanted to know if they should go ahead and complete it.

**A:** Yes, it will have to be completed at some point. This information could help with our initial assessment as we work through this process.

**Q:** Tonya Faler (MS Dept of Employment Security (MDES))

When will AMEX be ready for agencies/applications to use/accept?

**A:** Now. You can contact Lea Anne Culp @ 601-359-1338 or [culpl@dfa.state.ms.us](mailto:culpl@dfa.state.ms.us) for the form to complete.. We will work with you and AMEX to get this process in place.

**Q:** Jennifer Wentworth (MS State Tax Commission)

How does PCI DSS effect or relate to ACH transactions?

**A:** DFA is going to apply these same rules to ACH transactions in order to protect the consumer and the state. This information needs to be safeguarded just as much as the credit card information.

**Q:** Daryl Smith (MS Department of Environmental Quality)

There have been documented issues about the differences in public sector entities and retail entities accepting card payments. Has this been resolved?

**A:** Both DFA and the Consumer Protection Division of the Attorney General's Office are monitoring this on-going issue. A number of issues are related, including, but not limited to, issues of liability, issues regarding convenience fees and the need for those in the public sector, and standard government pricing. It was noted that AMEX has standard government pricing while VISA and MasterCard do not; however, VISA and MasterCard tend to authorize government pilot projects for tax collections, etc. MasterCard recently completed a successful IPO (initial public offering), and VISA is expected to issue one in early 2008. It is hoped that these actions will make the operating rules and guidelines more open and understandable.

**Q:** Rosina Echols (Department of Banking and Consumer Finance)

How do, or don't, honesty bonds cover us regarding PCI issues?

**A:** Honesty bonds provide only limited coverage. Cille has discussed employee versus agency liability with Greg Hardy, Director of the Office of Tort Claims, regarding insuring the State against issues such as these. One of the decision points is the question of intent: If an employee, in the course of their employment with the state, makes an honest error that causes a breach, such as exposure of personal financial information, etc, then that is one issue. However, if an employee commits fraud and/or abuse, the employee becomes personally liable. Greg has agreed to review our risk management efforts and any future contracts to ensure that the State is protected, and to assist us in meeting vendor requirements concerning the liability related to PCI DSS training of employees. Training of employees, as to their role and responsibilities in this area, will be part of the risk management requirements.

<b>Agency</b>	<b>Attendee(s)</b>
Agriculture and Commerce	Crystel James Joette Pickle
Arts Commission	Alesha Nelson
Banking and Consumer Finance	Rosina Echols Stacy Guynes Tina Smith
Board for Community and Junior Colleges	Debbie Borgman
Board of Bar Admissions	Glenda Middleton Linda Knight Miranda Armstrong
Board of Nursing	Dan Patterson James (Jim) Mack
Bureau of Narcotics	Carolyn Orr Miranda Holly
Dental Examiners Board	Leah Diane Howell
Education	Deborah Giles Linda Whitley
Emergency Management Agency	Wanda McAllister
Employment Security	Laronda Thompson Tonya Faler
Environmental Quality	Daryl Smith Debbie Wolfgram Janet Ray Mona Varner Yana Moore
Finance and Administration	Carol Wilson Cille Litchfield Clyde Murrell Dora Sisney Jim Hurst Lea Anne Culp Linda Jones Mary Ann Taylor Sharon Harper
Forestry Commission	Jennifer Head Rebekah Olander Robert Ponder Russell Jones
Health	Dick Johnson Marcia Williams

Human Services	Willie Fortner
Information Technology Services	Brian Norwood Mike Hatch Renee Murray Rick Grant
Insurance Department	Linda Chase Nancy Stuart
Library Commission	Elieen S. Wortham
Licensure for Professional Engineers/Surveyors	Debbie Bass Rosemary Brister
Medicaid	Anthony Terry Rudy Ware
Mental Health	Jackie Bailey Lisa Henick
Military Department	Evelyn Brandon Margaret Miller
Mississippi State Hospital	Don Dees
Public Safety	Marcy Rideout
Secretary of State	Cindy Crocker Karana Carroll Libby Cajoleas
State Fire Academy	Pam Ladner
Tax Commission	Jennifer Wentworth
Transportation	Christie Knight Jeff Whittington
Wildlife Fisheries and Parks	Alison English Audrey Bryant Curtis Thornhill Jason Thompson Michael Bolden
Workers' Compensation Commission	Inez Azain