Introduction: The purpose of the document is to give our financial institutions and retailers clients and colleagues guidelines on how they should approach PCI/EMV and other compliance areas such as ADA. This is not an official guide but an attempt to help bring clarity to the compliance requirements in each of these areas. Also we do reference specific resources, description and processes published by PCI, EMV and ADA that are available and key to all affected parties.

PCI...The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

The PCI Security Standards Council has published a large number of standards, guidelines and offers training and resources to all affected parties which include financial institutions and their subsidiaries, retailers who accept cards for payments, and other processors and organizations who handle payment account data. PCI also affects all manufacturers of ATMs and POS related authorization equipment, and online authorization processes.

It is important to note that the PCI Council DOES NOT validate or enforce any organization's compliance with its PCI Security Standards, nor does it impose penalties for non-compliance. These areas are governed by each of the payment brands and their partners. Accordingly, compliance requirements and deadlines are established and monitored by each of the 5 brand companies and below are the websites:

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: http://www.discovernetwork.com/merchants/
- JCB International: http://www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: http://www.mastercard.com/sdp
- Visa Inc: http://www.visa.com/cisp and Visa Europe: http://www.visaeurope.com/ais

PCI security for merchants and payment card processors is the vital result of applying the information security best practices in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment; for purposes of PCI compliance, their essence is three steps: Assess, Remediate and Report.

To **Assess** is to take an inventory of your IT assets and business processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data. To **Remediate** is the process of fixing those vulnerabilities. To **Report** entails compiling records required by PCI DSS to validate remediation and submitting compliance reports to the acquiring bank and global payment brands you do business with. Carrying out these three steps is an ongoing process for continuous compliance with the PCI DSS requirements. These steps also enable vigilant assurance of payment card data safety.

For more information on the process and how to get started visit:
https://www.pcisecuritystandards.org/security_standards/getting_started.php

PCI Compliance is critical to all parties, merchants, financial institutions, processors, etc., and is an ongoing process. Here is a link that explains the importance of compliance whether a large FI or small merchant: https://www.pcisecuritystandards.org/security_standards/why_comply.php

CashTrans has published a flyer which reviews the 12 requirements to insure your ATM Network is PCI compliant. Click on this link to download a copy: http://www.cashtrans.com/PCI_requirements.

Once you are engaged in PCI Compliance, you must check with each card brand that you accept or process to find out their exact compliance requirements. While most deadlines have passed for large merchants and processors, if is important to assess where your organization stands and the associated risks, as noted above.

EMV – "EuroPay MasterCard Visa" - The adoption of EMV or chip card technology will impact card issuers, merchants, ATM deployers and terminal manufacturers over the course of the next several years. While virtually the entire world has adopted this chip card technology to some degree and the U.S. has not. EMV is considered far more secure than magnetic-stripe cards because customer data is encrypted inside a chip, making it harder to hack. Most experts are convinced fraud has been reduced significantly as a result of EMV adoption.

EMV affects two major players in the merchant payments industry, namely merchants and their processors in the POS world. Also EMV adoption in the US will be again driven by the major card brand companies. The generally accepted target date for full implementation for POS and ATM is well into 2015, some brands are pressing for earlier adoption like MasterCard as early as April 15, 2013 but this only applies to Maestro transactions.

To obtain an excellent overview on EMV or chip card technology, visit EMVco LLC for a guide on EMV:
http://www.emvco.com/best_practices.aspx?id=217

With respect to most ATM manufacturers, EMV has widespread adoption outside the U.S. and the transition within the U.S. should be quite smooth with the key hurdle the replacement or modification of dip readers. One example of a manufacturer ready to fully support ATM deployers today is Diebold Corp. If you would like to review their status and support simply register and replay a recent Diebold webinar on EMV adoption in the U.S: http://pages.e.diebold.com/webinar-calendar

ADA – Americans with Disabilities Act that affects ATMs has been widely implemented across the U.S. by most financial institutions and major ATM deployers by the compliance date of March 15, 2012. However, there are a number financial institutions and deployers who are still in the conversion process and hopefully have protected themselves by documenting plans to complete the required ATM modifications in a timely manner.

The major risk of non-compliance is non-compliance lawsuits which have been documented across the country and can result in penalties in the hundreds of thousands of dollars.

To get review all the ADA ATM compliance requirements visit the following link:
http://www.ada.gov/regs2010/2010ADAStandards/2010ADAstandards.htm

Authored by Russ Schoper, Director of Marketing and Dan Bailey SVP Sales at CashTrans