

A close-up photograph of a hand holding a credit card. The card is dark blue or black with a signature strip that says "AUTHORIZED SIGNATURE". The background is dark and out of focus.

Deloitte.

Payment Card Security

*How effective is
your PCI program?*

January 31, 2008

Kieran Norton, Senior Manager
Security & Privacy Services, Deloitte & Touche LLP

Audit • Tax • Consulting • Financial Advisory.

Focus of the Presentation

PCI Overview

- Background
 - Current Environment
 - Key Considerations
-

This publication contains general information only and Deloitte & Touche LLP is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte & Touche LLP its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

PCI Overview: Background



What is the PCI DSS?

- The Payment Card Industry (PCI) Data Security Standard (DSS) represents a set of fundamental security requirements, industry tools and measurements that address the handling of sensitive (i.e., cardholder) information.
- The PCI DSS comprises six control objectives and 12 primary requirements. The six control objectives are:
 - 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 Program
- The PCI DSS program documentation also includes common auditing and scanning procedures, as well as a Self-Assessment Questionnaire.

PCI Compliance Programs

- Maintenance of the PCI DSS is overseen by the PCI Security Standards Council, an organization founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.
- While the PCI DSS serves as an industry standard, individual payment brands — and not the PCI Security Standards Council — are responsible for accepting or declining recommendations of compliance from Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs).
- Key payment brand compliance programs include:
 - Visa’s U.S.-based Cardholder Information Security Program (CISP) and the international Account Information Security (AIS) program
 - MasterCard’s Site Data Protection (SDP) program
 - American Express’ Data Security Operating Policy (DSOP)

PCI Compliance Validation

- PCI compliance is required by all entities that store, process, or transmit cardholder information.
- In order to be considered “PCI compliant,” an entity must comply with all of the requirements in the PCI DSS (either directly or through appropriate compensating controls).
- Compliance validation requirements vary depending on the payment brand program and the merchant or service provider level (e.g., Level 1 through 4).
- PCI level assignments are generally based on the number of transactions processed by the merchant or service provider; however, any merchant who experiences a breach that resulted in an account data compromise or is identified as a Level 1 merchant by any one of the payment brands, is automatically designated a Level 1 merchant by all payment brands.
- Merchants/service providers whose compliance validation requires on-site security audits and network scanning must engage PCI approved third-party Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs).
- An entity may be able to assess compliance with the PCI DSS through a singular review (and QSA); however, the entity would still be required to follow each payment brand’s respective compliance validation and reporting requirements.

Compliance Validation Requirements: Merchants

Merchant Compliance Validation Requirements				
Payment Brand	Level 1	Level 2	Level 3	Level 4*
Visa Cardholder Information Security Program (CISP)	<ul style="list-style-type: none"> • 6M+ transactions regardless of acceptance channel • Onsite security audit required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • 1-6M transactions • Self-assessment questionnaire required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • 20K-1M e-commerce transactions • Self-assessment questionnaire required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • Less than 20K e-commerce or 1M overall transactions • Self-assessment questionnaire recommended annually • Network scan recommended quarterly
MasterCard Site Data Protection (SDP) program	<ul style="list-style-type: none"> • 6M+ transactions regardless of acceptance channel • Onsite security audit required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • 1-6M transactions • Self-assessment questionnaire required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • More than 20K e-commerce, less than 1M total transactions • Self-assessment questionnaire required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • All other merchants • Self-assessment questionnaire required annually • Network scan required quarterly
American Express Data Security Operating Policy (DSOP)	<ul style="list-style-type: none"> • 2.5M+ transactions • Onsite security audit required annually • Network scan required quarterly 	<ul style="list-style-type: none"> • 50K-2.5M transactions • Network scan required quarterly 	<ul style="list-style-type: none"> • Less than 50K transactions • Network scan recommended quarterly 	N/A

* Although not required by the payment brands, **Acquirers** may request that its Level 4 (Level 3 under DSOP) merchants submit PCI DSS compliance validation.

Scope of Compliance Assessment

- For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:
 - All external connections into the merchant network (e.g., employee remote access, payment card company, third party access for processing, and maintenance)
 - All connections to and from the authorization and settlement environment (e.g., connections for employee access or for devices such as firewalls and routers)
 - Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS
 - A point-of-sale (POS) environment – The place where a transaction is accepted at a merchant location (i.e., retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
 - If there is no external access to the merchant location (i.e., by Internet, wireless, virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded.
- For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted, unless otherwise specified.

Scope of Compliance Assessment

- Merchants and service providers also are required to conduct a network-based PCI Security Scan.
 - Per PCI Requirement 11.2, “Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry” [i.e., a third-party PCI Approved Scanning Vendor (ASV)].
 - The scope of the scan includes all Internet-facing IP addresses; however, the scope can be reduced by:
 - Providing physical segmentation between the network segment handling cardholder data and other segments
 - Employing appropriate logical segmentation where traffic is prohibited between the segment or network handling cardholder data and other networks or segments
 - If an account data compromise occurs via an IP address or component not included in the scan, the merchant or service provider will be held responsible.

Compliance Deadlines and Fines

Visa's PCI Compliance Acceleration Program (CAP)

- As of March 31, 2007, Visa is fining Acquirers whose Level 1 and 2 merchants are storing full track, CVV2, or PIN data (i.e., "prohibited data"). Fines are up to \$10,000/month, subject to escalation in the event that material progress toward compliance is not made in a timely manner.
- Deadlines for overall PCI Compliance are 9/30/2007 (Level 1) and 12/31/2007 (Level 2).
- Visa will issue fines ranging from \$5,000 to \$25,000/month to Acquirers per each merchant that does not meet the overall PCI compliance deadlines.
- It is highly likely that Acquirers will allocate CAP fines to the respective merchant.
- Acquirers whose merchants do not meet the PCI compliance deadlines may not be eligible for the best tiered interchange rates for that merchant.

AMEX's DSOP

Fines will be issued if a merchant cannot provide compliance validation documentation by their assigned compliance deadline (10/31/2007 for Level 1 merchants). Fines are set at:

- \$50,000 if documentation is not received by the first deadline.
- An additional \$150,000 fee if documentation is not received within 30 days of the first deadline.
- An additional \$200,000 fee if documentation is not received within 60 days of the first deadline.

MasterCard's SDP

Reserves the right to "levy a non-compliance assessment on the responsible MasterCard member" if merchants do not meet SDP requirements.

PCI Overview: Current Environment



Credit Card Primer

What data is stored on a credit card and why is it important?



Magnetic Stripe (i.e., “track data”)

- Contains sensitive data including cardholder name, account number, expiration date, CVV, and PIN verification value (PVV).
- Full track information cannot be stored.
- CVV and PVV values cannot be stored.
- Elements of the track that may be retained as required by business needs are: cardholder name, account number, expiration date and service code.
- If stored and compromised, the data can enable production of counterfeit cards.

Card Validation Value or Code (e.g., CVV2, CVC2, CID, CAV2)

- A 3 or 4 digit code that helps mail order/telephone order (MO/TO) and e-Commerce merchants validate that the customer has the card in their possession and that the account is legitimate.
- This information cannot be stored.
- If stored and compromised, the data can enable fraudulent online transactions.

PIN values key entered into PIN PAD devices for debit transactions also cannot be stored, even if encrypted (e.g., PIN blocks).

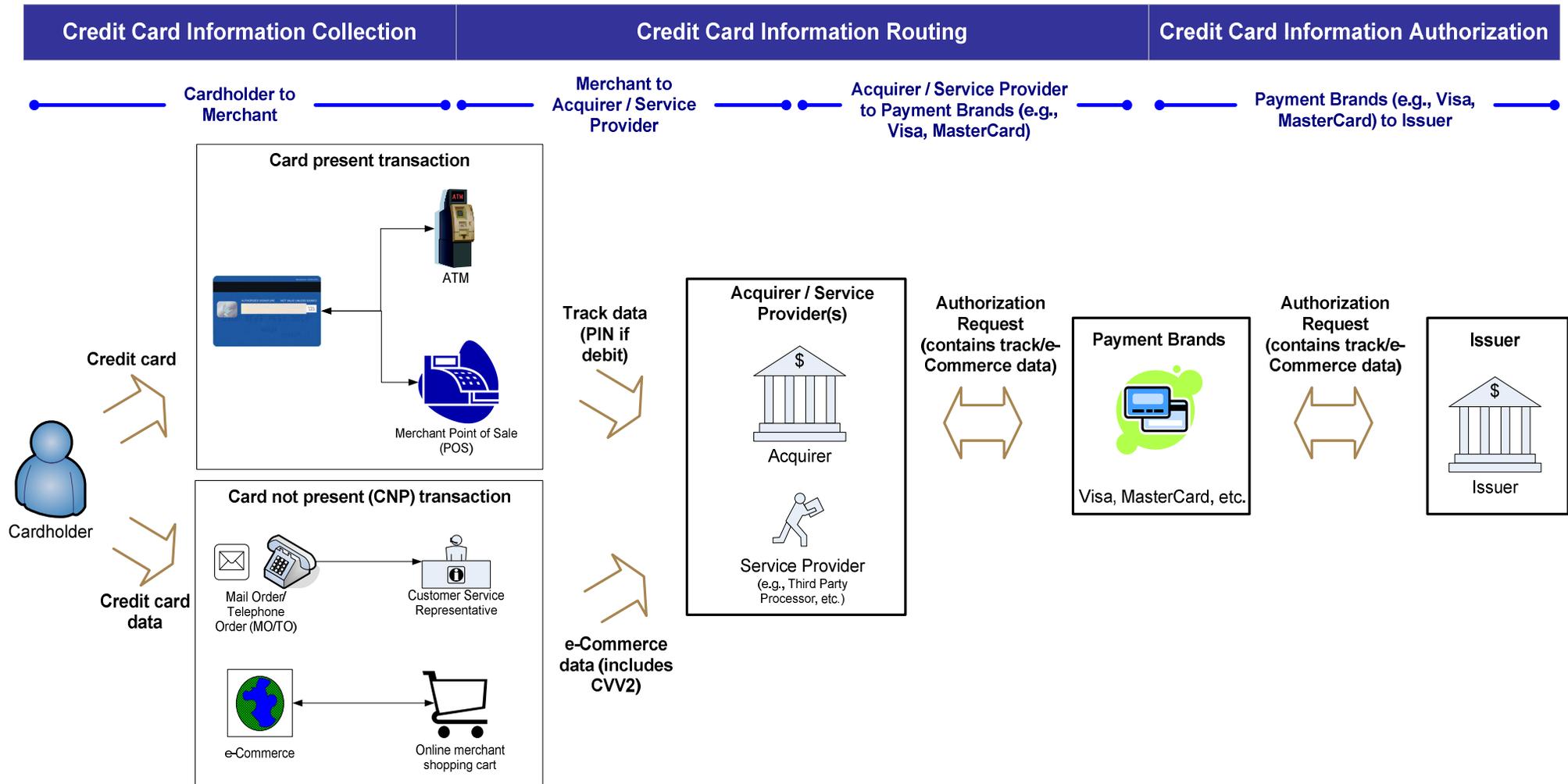
Credit Card Primer

Who are the key credit card entities?

Entity	Description
Merchant	Any business that, having met the qualification standards of a payment brand and having been approved by any Acquiring member, accepts payment cards in exchange for goods and services.
Acquirer	Payment brand member that maintains relationships and accounts for merchants that accept payment cards. Serves as the intermediary figure between merchants and the payment brands.
Service Provider (e.g., Processor, Gateway, Hosting Provider)	<p>Business entity that is not a payment brand member or a merchant directly involved in the processing, storage, transmission, and switching of transaction data and cardholder information or both.</p> <p>This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data (e.g., service providers that provide managed firewalls, IDS and other services, hosting providers).</p>
Payment Brand (e.g., Visa, MasterCard)	Processing organization that licenses members and merchants to issue and accept credit cards, respectively. The organization serves as an intermediary between Acquirers and Issuers.
Issuer	The financial institution (i.e., a licensed member of a payment brand) that holds contractual agreements with and issues cards to cardholders. Also responsible for managing cardholder accounts and approving authorizing requests.

Credit Card Primer

How does a transaction get processed?



Common Schemes and Attacks

- Examples of traditional credit card-based schemes and attacks include:
 - **Skimming:** Using a small device to steal information from a card's magnetic stripe. This information is used to create counterfeit cards and make fraudulent purchases.
 - **Postal theft:** Intercepting new or renewed credit cards in transit to the appropriate cardholder.
- Over time, traditional attacks have “improved” – more professional perpetrators (e.g., organized crime syndicates) executing more sophisticated attacks, increasing “scope of compromise,” robust global fraud networks, and increasingly complex fraud schemes. Examples include:
 - **Gift card fraud:** A 2nd generation fraud scheme in which stolen credit card data is used to purchase gift cards to “extend the life of the card” after the original card is reported missing.
 - Gift cards also used in combination with skimming activities – perpetrator skims card in the store, makes a duplicate, waits for a customer to activate the card.
 - Counterfeit gift cards can be sold on gift card swap sites (e.g., cardavenue.com, swapagift.com) that allow customers to buy and trade gift cards online.
 - **Credit card manufacturing websites:** Underground Websites that market illegally manufactured credit cards using stolen credit card data.
 - Shadowcrew.com trafficked in at least 1.7M stolen credit card numbers and caused total losses in excess of \$4M through illegally manufactured credit cards.
 - Websites commonly operated by organized crime syndicates.
- Both traditional and contemporary schemes and attacks are alive and well today.

Industry View

- Payment card fraud has reached a new level of intensity and consumer awareness due to a series of significant, recent public security breaches, including:
 - TJX (TJ Maxx): Late 2006 compromise of more than 94 million credit and debit card numbers over a period of more than 18 months
 - Organized Skimming: Thirteen individuals indicted on 4/20/07 on charges related to a U.S. restaurant-based organized credit card-skimming operation (i.e., 40 restaurants across five states) that has resulted in more than \$3 million worth of fraudulent activity
 - CardSystems: Compromise in 2005 that exposed more than 40 million credit card numbers
 - DSW: Compromise in 2005 that exposed more than 1.4 million credit card numbers
- Impacts of card breaches include, but are not limited to:
 - Significant brand impact associated with public notification of data breach
 - Fines levied by federal agencies (i.e., FTC)
 - Payment brand fines and dispute resolution costs
 - Lawsuits
 - Prevailing industry and customer perception of correlation between data breach and identity theft

Focus on PCI

- The increase in frequency and size of data breaches, as well as escalating counterfeit credit card fraud, has intensified scrutiny around how cardholder data is protected.
- The PCI DSS focuses on this issue through prescriptive requirements that target protection of cardholder data, especially within retail environments.
- As a result, the industry presence and relevance of the PCI DSS continues to grow:

Payment brands are instituting more significant countermeasures to non-compliance (e.g., fines, termination of card acceptance agreements).

Certain states have or are considering legislation that is in alignment with or specifically references PCI compliance (e.g., Minnesota's Plastic Card Security Act).

Various payment brand standards have now consolidated into the PCI DSS, which serves as the centralized foundation for compliance with the individual payment brand programs.

The PCI Security Standards Council is comprised of stakeholders from the major payment brands. The focus of the council includes broad adoption of the PCI DSS and active participation from all payment processing stakeholders.

Merchant Compliance Status

Visa U.S.A. Cardholder Information Security Program (CISP) PCI DSS Compliance Validation Update as of 9/30/07*

CISP Validation Category (Visa transactions / year)	Population	Estimated % of Visa Transactions	PCI DSS Compliance Validated***	Initial Validation Submitted / Remediating	Initial Validation In Progress	Pending Commitment
Level 1 Merchants** (> 6M)	327	50%	65%	35%	0%	0%
Level 2 Merchants** (1 – 6M)	720	13%	43%	42%	15%	0%
Level 3 Merchants (e-commerce only 20,000 – 1M)	2503	< 5%	55%	21%	22%	2%

* Validation statistics are based on merchant compliance reporting provided by acquirers.

** Includes Level 1 and Level 2 merchants identified from 2004 through 2006, which are required to validate by 9/30/07 and 12/31/07 respectively. Level 1 and Level 2 merchants identified as such in 2007 must validate compliance by 9/30/08 and 12/31/08 respectively.

*** Noteworthy, 99% of Level 1 and 2 merchants confirmed that they do not store prohibited data. Acquirers of Level 1 and 2 merchants that continue to store prohibited data are subject to monthly fines.

Source: Visa “Merchant PCI DSS Compliance Update” (available at http://usa.visa.com/merchants/risk_management/cisp_merchants.html)

PCI Overview: Key Considerations



Common Compliance Challenges

- Based on our work with clients, the following are common issues encountered during compliance assessment and remediation:
 - Point of Sale (POS) systems store magnetic stripe data by default (3.2) or are otherwise non-compliant
 - Cardholder data is not encrypted in storage (3.4)
 - Access to cardholder data is not logged and may not be technically feasible (10.2.1)
 - Network segmentation is not implemented (1.3)
 - Unprotected wireless connections (2.1.1)
 - Inability to patch appliances and applications
 - File integrity monitoring not implemented (11.5)
- Best practice until June 30, 2008 after which it will become a requirement: Ensure that all web-facing applications are protected against known attacks by applying either of the following:
 - Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
 - Installing an application layer firewall in front of web-facing applications

On the Road to Compliance

- Understand your level designation and whether it might change, related due dates and acquirer expectations across all card brands.
- Focus on building relationships with your acquirer(s) and key vendors (e.g. POS vendors, service providers); they will be quite important.
- Understand and communicate your electronic payments strategy; it will drive many of the decisions you make when evaluating compliance solution options.
- Integrate the PCI DSS requirements into your security program; do not manage them separately.
- Conduct a data flow analysis and system “inventory” effort to understand the complete lifecycle of the (cardholder) data you wish to protect and be certain to challenge what you are told.
- Prioritize (i.e., risk rank) critical systems, applications and components, conduct a security review, identify gaps, and manage remediation from an enterprise perspective.
- Take a strategic approach to remediation and consider all of the alternatives (e.g., data masking, data removal, “footprint” reduction, outsourcing, compensating controls).

Q&A



About Deloitte & Touche LLP's Security & Privacy Services

- The ongoing mission of Security & Privacy Services is to work with our clients to shape the advancement and evolution of security solutions. By working together, we can improve enterprise security and value, bring new solutions to market and develop risk aware programs and processes.
- The Security & Privacy Services professionals of Deloitte & Touche LLP are uniquely positioned to design, develop, and implement industry-leading information security solutions for businesses. We bring together many years of industry experience with the innovation and knowledge of nearly 1,500 professionals who deliver a complete range of security and privacy services across all industries.
 - Application Security/Integrity
 - Business Continuity Management
 - Identity & Access Management
 - Infrastructure & Operations Security
 - Privacy & Data Protection
 - Security Management
 - Vulnerability Management
- We offer comprehensive customized solutions that will help our clients maximize opportunities and master their most pressing and complex challenges. We value our clients and commit ourselves to their success.

Contact Information

Russell Jones

Principal

Deloitte & Touche LLP

rujones@deloitte.com

+1 415 783 5054

Kieran Norton

Senior Manager

Deloitte & Touche LLP

kinorton@deloitte.com

+1 415 783 5382

References

- PCI DSS Council:

Overview: <https://www.pcisecuritystandards.org/tech/index.htm>

Glossary of Terms: <https://www.pcisecuritystandards.org/tech/glossary.htm>

Qualified Security Assessors (QSAs):

https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

Approved Scanning Vendors (ASVs):

https://www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm

- Visa:

CISP Overview: http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp

Payment Application Best Practices (PABP):

http://usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc

What To Do If Compromised:

http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

References

- Visa (cont):

List of CISP Compliant Service Providers:

http://usa.visa.com/download/merchants/cisp_list_of_cisp_compliant_service_providers.pdf?it=c/merchants/marketing_center/merchant_resources/tips_tools_downloads.html|CISP%20Compliant%20Service%20Providers%20List

Validated Payment Applications:

http://usa.visa.com/download/merchants/validated_payment_applications.pdf?it=c/merchants/marketing_center/merchant_resources/tips_tools_downloads.html|Validated%20Payment%20Applications

- MasterCard:

SDP Overview: <http://www.mastercard.com/us/sdp/index.html>

- AMEX:

DSOP Overview:

https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 150,000 people worldwide, Deloitte delivers services in four professional areas — audit, tax, consulting, and financial advisory services — and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the United States, Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 40,000 people in more than 90 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at www.deloitte.com

Copyright © 2007 Deloitte Development LLC. All rights reserved.

Member of
Deloitte Touche Tohmatsu