MERCHANT SERVICES, INC.

attention: **Critical Security ALERT**

Fall 2005

What Every Merchant Needs to Know About Consumer Data Security

Your customers want assurance that their credit card account information is safe. But offering your customers a safe and secure way to pay is more than just a good business practice—it's a requirement. Every merchant who touches credit card account information is responsible for safeguarding that information and can be held liable for security compromises if they have not taken the required precautions.

To help merchants understand and adhere to their security regulations, Visa and MasterCard have aligned the compliance levels and validation requirements of their cardholder data security programs (CISP and SDP), creating the Payment Card Industry (PCI) Data Security Standard. The program is intended to protect cardholder data—wherever it resides—ensuring that banks, merchants and service providers maintain the highest information security levels.

Key Deadlines for Demonstrating Compliance

Deadline	Merchant Level	Requirement
Passed	Level 2 Merchants	Merchants must already have fulfilled their compliance obligation. (Contact your relationship manager or call the number on your statement with questions.)
Passed	Level 3 Merchants	Merchants must already have fulfilled their compliance obligation. (Contact your relationship manager or call the number on your statement with questions.)
Passed	All Merchant Levels	All merchants found to be storing full track data who have not corrected the issue are subject to enforcement. Full track data is defined as data encoded in the magnetic stripe used for authorization during a card present transaction. Merchants must not retain full magnetic stripe data subsequent to the transaction authorization.
Dec. 31, 2005	Level 1 Merchants	Most Level I merchants must provide a ROC that indicates full compliance with all PCI standards. (Contact your relationship manager for validation or call the number on your statement with questions.)
Passed Compliance required, Validation optional.	Level 4 Merchants	No current requirement. We urge Merchants to complete the compliance recommendations to help avoid security compromises.

Does this apply to me?

The PCI Data Security Standard Program applies to all U.S. entities that store, transmit or process cardholder data (i.e., Visa, MasterCard, American Express, Discover), regardless of payment channel (online, mail/telephone orders or "brick and mortar"). Additionally, these security requirements apply to all "system components," which are defined as "any network component, server or application included in, or connected to, the cardholder environment".

Why do I have to go through the compliance process?

The simple answer is to avoid potential fines that the card brands may levy. The more important reason is to protect your customers' confidential information and to safeguard your valuable reputation.

The card brands have set fines schedules for companies that are not compliant with the security programs:

Visa Non-Compliance Fees

First Violation	up to $50,000
Second Violation	up to $100,000
Third Violation	up to Management Discretion
Failure to Report a Compromise	up to $100,000
Egregious Violation	up to $500,000

MasterCard Non-Compliance Fees

Level 1 Merchants (more than 6 million MasterCard or Visa transactions per year)	Up to $100,000 and if not compliant after 60 days, additional fines of $10,000 per day not to exceed $500,000
Level 2 Merchants (150,000 - 6,000,000 MasterCard or Visa ecommerce transactions per year)	Up to $50,000 and $10,000 per day after 60 days, not to exceed $500,000
Level 3 Merchants (20,000 - 150,000 MasterCard or Visa ecommerce transactions per year)	Up to $25,000 and $10,000 per day after 60 days, not to exceed $500,000

Visa USA, Visa Canada and MasterCard have warned that they may restrict or terminate the merchant's or service provider's acceptance privileges for issues of non-compliance.

Even more importantly in the long run, your customers' trust and loyalty depend on it. Many consumers are becoming more and more aware of security relating to their personal information. Your compliance demonstrates that you are protecting your customers' personal data. A breach in security may cause irreparable damage to the relationships you have built with your customers, and ultimately negatively impact your bottom line. Is that a risk you are willing to take?

How do I ensure my company is compliant?

Visit the card brands' websites to view their compliance standards, which include:

- building and maintaining a secure network
- protecting cardholder data
- implementing strong access control measures

Once I become compliant, how long am I considered compliant?

Please be advised, once you are considered compliant, if you are a level 1, 2 or 3 merchant, we must register your company with MasterCard. If your company is storing credit card information, MasterCard will charge us with an annual $200 registration fee, which we will pass on to you. You must maintain compliance throughout the year. If your company suffers a security incident and is found to be operating in a non-compliant manner, your company will be subject to fines and other penalties.

What are the compliance deadlines?

The compliance deadlines vary by card brand and the number of credit card transactions your business processes. This bulletin includes a table that defines the four merchant levels and applicable deadlines. While this information is current as of this printing, we strongly recommend you visit the Visa and MasterCard compliance sites on a regular basis to find the latest information on compliance.

Where can I obtain additional information about the compliance programs?

Additional information on Security Programs can be found by searching "cardholder security" at the following websites:

- www.visa.com
- www.mastercard.com
- www.discovercard.com
- www.americanexpress.com

PCI Security Standards

The Payment Card Industry (PCI) Data Security Standard contains 12 requirement categories that are grouped into six general headings. The complete Payment Card Industry Data Security Standards are available for download from the MasterCard and Visa websites listed previously. The six general headings and 12 requirements are:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect data.
Requirement 2: Do not use vendor-supplied defaults for system passwords and security parameters.

Protect Cardholder
Requirement 3: Protect stored data.
Requirement 4: Encrypt transmission of cardholder data and sensitive information across 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 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.

These standards apply to all Members (financial institutions), merchants and service providers (a third party who provides payment-related services to merchants) that store, process or transmit cardholder data. Additionally, these security requirements apply to all "system components," which are defined as any network component, server, or application included in, or connected to, the cardholder environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including internal and external (web) applications.

PCI Merchants

Merchant Level	Selection Criteria	Required Actions to Validate Compliance
Level I	1. Any merchant, regardless of acceptance channel, processing over 6,000,000 Visa or MasterCard transactions per year. 2. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. 3. Any merchant that Visa or MasterCard, at their sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to their systems.	1. Annual on-site security audit completed by a Qualified Independent Security Assessor or Internal Audit Staff if signed by company officer. 2. Quarterly network scan conducted by a qualified independent scan vendor.
Level II	Any merchant processing 150,000 to 6,000,000 Visa or MasterCard ecommerce transactions per year. An ecommerce transaction is any transaction obtained via an outwardly facing web page.	1. Annual PCI Self-Assessment Questionnaire validated by the merchants. 2. Quarterly network scan conducted by a qualified independent scan vendor..
Level III	Any merchant processing between 20,000 to 150,000 ecommerce Visa or MasterCard transactions. An ecommerce transaction is any transaction obtained via an outwardly facing web page.	1. Annual PCI Self-Assessment Questionnaire validated by the merchants. 2. Quarterly network scan conducted by a qualified independent scan vendor.
Level IV	Any other merchant, regardless of acceptance channel.	1. Recommended Annual PCI Self-Assessment Questionnaire validated by the merchant. 2. Recommended quarterly network scan conducted by a qualified independent scan vendor.

Validation and Reporting Requirements

Compliance registration and validation requirements for merchants still vary between Visa and MasterCard.

Level 1 Merchants Both Visa and MasterCard now require a Report on Compliance (ROC) and documentation of satisfactory perimeter scan results. Merchants should forward these results to us to complete the validation and registration process.

Level 2 and 3 Merchants Both Visa and MasterCard require a completed annual PCI Self-Assessment Questionnaire and successful quarterly scans. Merchants should forward these results to us to complete the validation and registration process.

Level 4 Merchants Both Visa and MasterCard require these merchants to meet the compliance requirements. However, merchants are not required to register with Visa or MasterCard at this time.

Helpful Terms and Definitions

Acquirer. A bankcard association member that initiates and maintains relationships with Merchants that accept Visa or MasterCard cards.

Cardholder. The customer to whom a card has been issued or the individual authorized to use the card.

Cardholder Data. All personally identifiable data about the cardholder and relationship to the Merchant (i.e., account number, expiration date, data provided by the Merchant, other electronic data gathered by the merchant/agent and so on). This term also accounts for other personal insights gathered about the cardholder (i.e., addresses, telephone numbers, and so on).

CISP. Visa's Cardholder Information Security Program establishes requirements for safeguarding personal cardholder information.

Compliance. Refers to operating within the bounds of the relevant card brand standards.

Compromise. An intrusion into a computer system where unauthorized disclosure, modification or destruction of cardholder data may have occurred.

Ecommerce Transaction. Any transaction obtained via an outwardly facing web page.

Encryption. The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

Magnetic Stripe Data (Full Track Data). Data encoded in the magnetic stripe used for authorization during a card present transaction. Entities may not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/CVV and Visa reserved values must be purged; however, account number, expiration date and name may be extracted and retained.

Payment Card Industry Data Security Standard. The alignment between the Visa and MasterCard compliance levels and validation requirements of their cardholder data security programs (CISP and SDP).

PCI Self-Assessment Questionnaire. The questionnaire that all Level 2 and 3 Merchants are required to complete and submit to their Acquirer.

Perimeter Scan. A non-intrusive test which involves probing external-facing systems and reporting on the services available to the external network (i.e., services available to the Internet).

ROC. The Report on Compliance required by MasterCard and Visa for every Level 1 Merchant.

SDP. MasterCard's Site Data Protection program establishes requirements for data security and helps Merchants proactively protect themselves and the overall payment system against the threat of compromises.

Truncation. The practice of removing a data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.

Vulnerability Scan. An automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool remotely reviews networks and Web applications based on the external-facing Internet protocol (IP) addresses. Scans identify vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network.