OutSecure, Inc.
'Survival of the Securest'

Ensuring Compliance with Credit Card Security Policies

Merchants, data processors, and any other vendors that manage credit card holder data today must adhere to strict policies for ensuring that data is secure at all times.
Whether they're working with American Express, Discover, MasterCard, Visa, or any other credit card vendor, these organizations face steep penalties, including fines and lost business, if this data is stolen. OutSecure can help address many of the critical security challenges of adhering to credit card issuer policies pertaining to data privacy within the enterprise.

In an effort to combat data theft and better ensure the protection of cardholder data, all of the major credit card issuers have formulated detailed security programs, such as:

- American Express Data Security Operating Policy (DSOP)
- Discover Information Security and Compliance (DISC) program
- MasterCard Site Data Protection (SDP) program
- Visa International Account Information Security (AIS) program
- Visa USA Cardholder Information Security Program (CISP)

In addition, in late 2004, Visa and MasterCard have aligned their programs in the Payment Card Industry (PCI) Data Security Standard. While all of these policies feature mandates on everything from changing employee passwords regularly to deploying firewalls, many rules focus on the security of data while it is stored within the enterprise.

OutSecure works to protect data within the enterprise, and works with clients to provide solutions to protect card holder data.

Achieving Data Privacy with OutSecure

OutSecure can help enterprises secure critical data that matters most to their business, including credit card numbers, social security numbers, and other critical, personally identifiable records. Following are a few key areas of credit card vendor security requirements and an overview of how OutSecure addresses them.

Protecting Data Privacy with Comprehensive Encryption

Encrypting sensitive data at rest is one of the keys to achieving compliance with credit card security policies. According to the PCI guidelines, here's why:
"Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle."
Each of the issuer programs offer specific guidance with respect to encryption, and specifically encryption of data at rest. For that processors must, "Encrypt all stored payment data using triple DES encryption."
MasterCard's E-commerce Self-Assessment Requirements feature a section on database security, stating…
"Applications and databases must store all sensitive cardholder details in an encrypted form. The keys used to encrypt the data must be of sufficient strength, based on current industry standards, such as 128-bit triple Data Encryption Standard (DES) or other algorithm."

Visa's CISP rules include mandating that passwords are encrypted, and that cardholder data is encrypted by…
"one-way cipher (hash indexes) such as SHA-1 (not MD5), Truncation, Simple ciphers, index tokens and PADS, strong cryptography such as PGP or Triple-DES with associated key management processes and procedures."

Finally, Discover mandates that "Card data that is stored and/or transmitted must be done so in an
encrypted fashion."

Restricting Physical Access to Data—and the Keys that Protect it

Even if data is encrypted, that data is still only as secure as the cryptographic keys used to do the encryption. That's why card guidelines specify a range of precautions for securing cryptographic keys. PCI guidelines state organizations should "store keys securely in the fewest possible locations and forms."

Control Online Access to Data

American Express, MasterCard, and Visa also mandate that precautions are taken to eliminate unauthorized online access to data. American Express requires that organizations "issue a unique ID to each person with computer access to payment data" and "require two-person control to access encrypted data."

MasterCard's best practice guidelines for "Access Control and Accountability" advocate "twofactor authentication," meaning, in addition to user name and password, users are authenticated by an additional means as well.

Visa's CISP mandates that at least one of the following methods are used to "authenticate all non-consumer users when accessing cardholder information": unique user name and password, token devices (i.e., SecureID, certificates, or public key), or biometrics.
OutSecure advises comprehensive capabilities for managing user access, authentication, and access control.
Further,We recommend separation of duties. For this reason, a single staff member performing key management functions should never have sole access to encrypted data, the platform operation, maintenance responsibilities, or other support functions…

Monitoring and Auditing Resource Access

Credit card policies also center on the ability to monitor and audit the access of protected resources.
American Express requires "the ability to track employee access to payment data through the use of unique IDs" and that organizations be "prepared to provide audit reports to American Express or allow American Express audits."
MasterCard's best practice guidelines for "Access Control and Accountability" urge the logging of all successful and unsuccessful requests.
Visa's CISP requires that "access to all audit trails logged on all critical systems."
OutSecure, advises all cryptographic functions and access performed by all users and administrators are also securely logged, stored, and available for reporting purposes.

Selectively Protect Sensitive Data

Today, organizations are contending with ever-increasing volumes of data—data that must be stored, accessed, transmitted, and secured, all while it is being used by an increasingly distributed network of employees, partners, and customers.
The credit card security policies outlined above focus on securing cardholder data, and typically vendors must manage a host of associated data that doesn't need to be protected.
OutSecure works with clients on intelligent security capabilities that enable organizations to select only the confidential information that needs to be secured.